MAGTF STAFF TRAINING PROGRAM

SEMPER FIDELIS

DOCEMUS PRIMAM ACIEM

Windows 2003 Server

Course Outline

- WINDOWS 2000 PRODUCT LINE
- PLANNING
  - Installation methods
  - Server Prep
  - Hardware Requirements
  - NTFS/RAID
  - Workgroup v.s. Domain
- INSTALL PHASES
- CONFIGURATION
  - Active Directory Re-Cap
  - DCPROMO lab
  - Site and Subnet lab
  - ADI DNS lab

Course Outline Cont.

- DFS
  - Functions
  - Replication
- USER MANAGMENT
  - The MMC
  - User Account
- GROUPS
  - Types
  - Creating
- GPO’s
- SERVICES
- DISASTER RECOVERY
- ADVANCED TOPICS ??

WINDOWS 2003 PRODUCTS

W2K3 Basics

- The Windows Server Family
- Windows Architecture
- Underlying Technologies
- Review
- Quiz Yourself

W2K3 Product Line

- Windows Server 2003—Standard Edition
- Windows Server 2003—Web Edition
- Windows Server 2003—Enterprise Edition
- Windows Server 2003—DataCenter Edition

W2K3—Standard Edition

Windows Server 2003 has the following limitations:

- A maximum of four microprocessors may be used.
- No more than 4GB of memory is allowed. Of that 4GB, the operating system always reserves 2GB for its own use, allowing applications on the server to share the remaining 2GB.

W2K3—Web Edition

The Web Server edition is optimized for Microsoft’s Internet Information Services (IIS) Web server platform. The Web Server edition does not support some advanced services, including:

- Advanced network security features like Internet Authorization Server
- Fax services
- Terminal services

W2K3—Enterprise Edition

It provides all of the same features and capabilities as the standard edition and adds the following:

- Support for up to eight microprocessors in a server.
- Expanded memory support that reserves only 1GB of memory for the operating system, allowing applications on the server to share the remaining 3GB.
- The ability to create clusters of two servers.

W2K3—Datacenter Edition

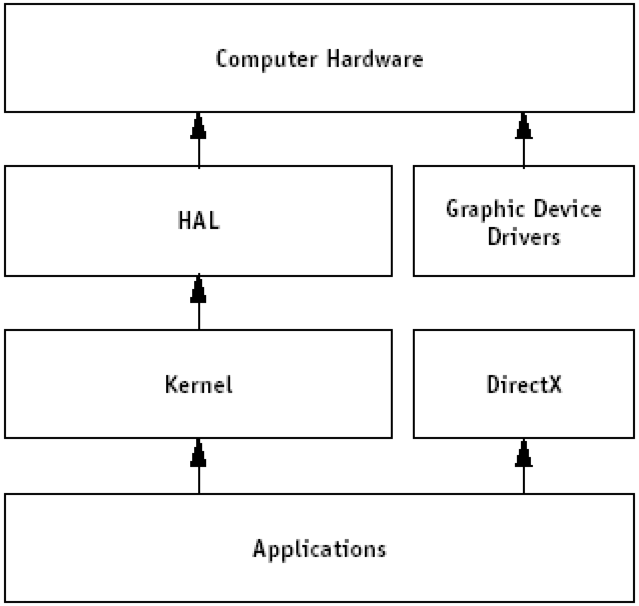
Like the Enterprise Server edition, Datacenter Server builds upon the standard Windows Server 2003 edition and adds the following features and capabilities:

- Support for up to 32 processors in a single server
- Support for up to 64GB of memory
- Support for clusters of up to four servers

Windows Architecture

- Windows Server 2003 is a multithreaded, multiprocessing, multitasking operating system.
- Windows Server 2003 also offers compatibility with an enormous array of hardware devices, allowing the operating system to interact with storage devices, scanners, networks, and many other types of peripherals.

Operating system architecture



Application architecture

- ***Multitasking***
  - *Multitasking* refers to Windows’ ability to run multiple tasks at the same time.
- In reality, computer’s processor can’t run multiple tasks at once.
  - Windows kernel includes a *task scheduler.*
    - keeps tracks of all the applications currently running on the computer and assigns each of them a *time slice.*

Multithreading

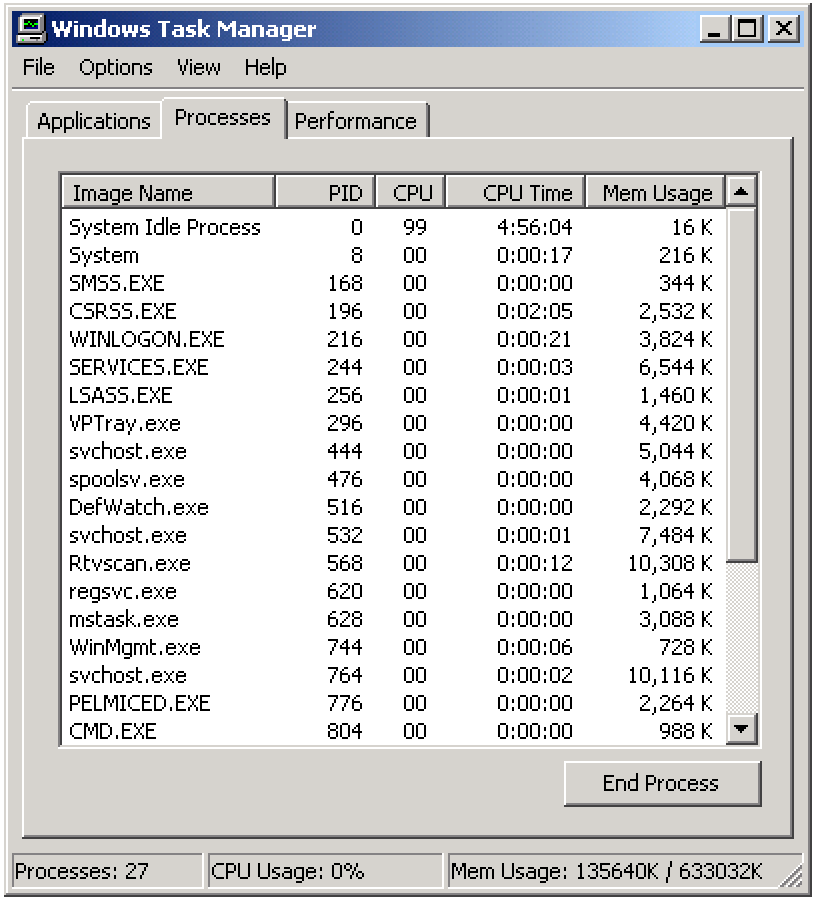


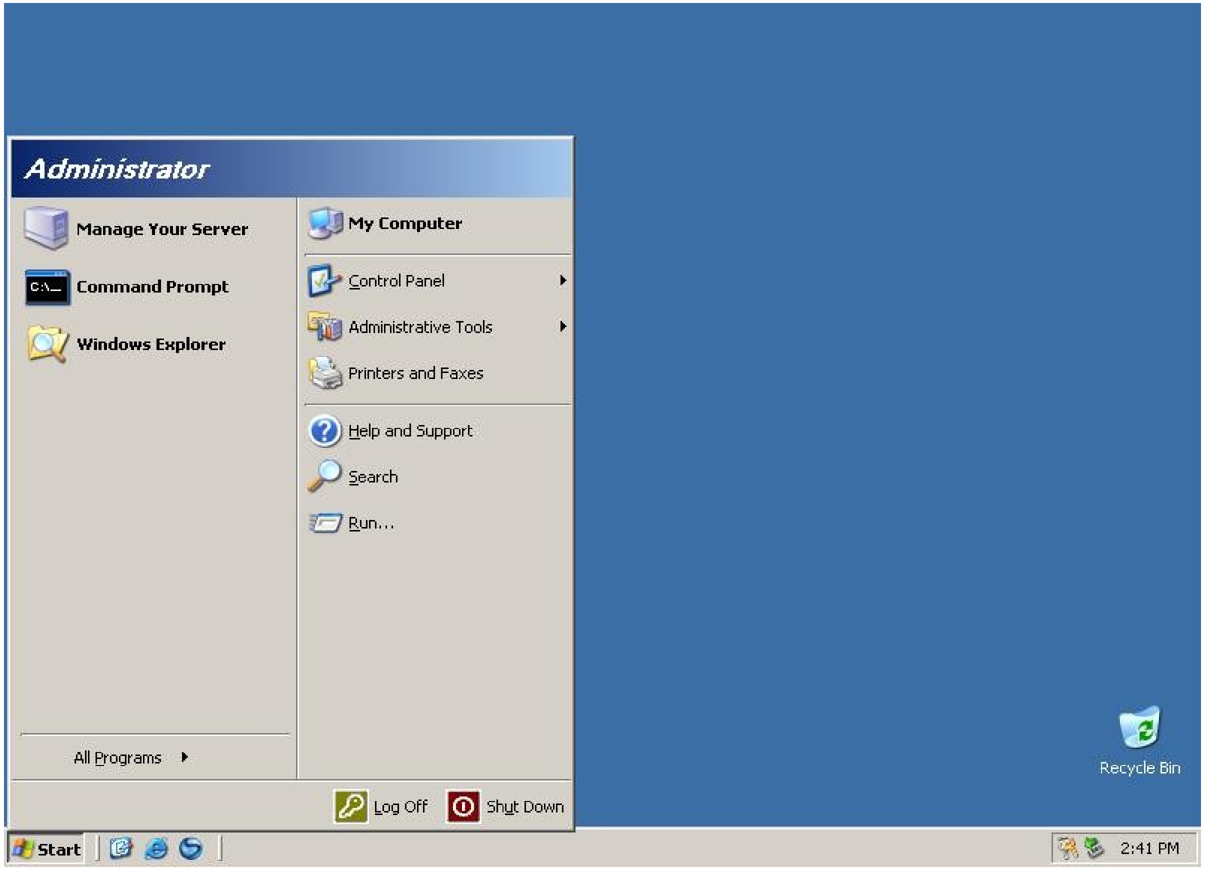
Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	99	4:56:04	16 K
System	8	00	0:00:17	216 K
SMSS.EXE	168	00	0:00:00	344 K
CSRSS.EXE	196	00	0:02:05	2,532 K
WINLOGON.EXE	216	00	0:00:21	3,824 K
SERVICES.EXE	244	00	0:00:03	6,544 K
LSASS.EXE	256	00	0:00:01	1,460 K
VPTray.exe	296	00	0:00:00	4,420 K
svchost.exe	444	00	0:00:00	5,044 K
spoolsv.exe	476	00	0:00:00	4,068 K
DefWatch.exe	516	00	0:00:00	2,292 K
svchost.exe	532	00	0:00:01	7,484 K
Rtvscan.exe	568	00	0:00:12	10,308 K
regsvc.exe	620	00	0:00:00	1,064 K
mstask.exe	628	00	0:00:00	3,088 K
WinMgmt.exe	744	00	0:00:06	728 K
svchost.exe	764	00	0:00:02	10,116 K
PELMICED.EXE	776	00	0:00:00	2,264 K
CMD.EXE	804	00	0:00:00	988 K

Processes: 27 | CPU Usage: 0% | Mem Usage: 135640K / 633032K

Multiprocessing

- On a computer with more than one processor, Windows is truly capable of working on more than one thing at a time.
- ***Underlying Technologies***
- ***Networking***
- ***Security***
- ***Services***
- ***Graphical user interfaces (GUIs)***

The classic Windows GUI



Review

In this session, you learned about the four editions of the Windows Server 2003 family:

- Windows Server 2003—Standard Edition
- Windows Server 2003—Web Edition
- Windows Server 2003—Enterprise Edition
- Windows Server 2003—Datacenter Edition

You also learned about Windows' operating system and application architecture, including Windows' ability to perform multiprocessing, multitasking, and multithreading.

Finally, you learned about many of the basic technologies that Windows is built on, including TCP/IP, Windows' security model, and its graphical user interface, or GUI.

QUIZ YOURSELF

1. Which edition of Windows Server 2003 introduces the ability to create server clusters?

2. What is the main reason Datacenter Server is the most reliable edition of Windows Server 2003?

3. What part of Windows is responsible for interacting with a computer's hardware?

4. What part of Windows decides which tasks and threads are executed by the computer's processors?

5. What is the native networking protocol for Windows Server 2003?

PLANNING

Installing W2K3

- Installation Methods
- Performing an Installation
- Upgrading from Prior Versions of Windows
- Product Activation
- Headless Servers
- Review
- Quiz Yourself

Installing W2K3

- How to perform an attended installation
- How to create an unattended installation
- How to upgrade from prior versions of Windows Server
- How to perform a “headless server” installation
- How to perform product activation

Installation Methods

Windows Server 2003 offers three basic types of installation:

- A standard CD-based installation enables you to install the operating system from a CD-ROM drive, or even from a DVD-ROM drive, if you have one.
- A network-based installation doesn’t require you to have a CD-ROM drive. Instead, the installation is run from a copy of the installation CD, which is located on a networked file server.
- A RIS-based installation uses Remote Installation Services, or RIS, to install the operating system without using a CD or a copy of a CD.

Install 2003 Server Preparation

- **Check Hardware Compatibility List (HCL)**
  - One or more processors with a recommended minimum speed of 550 MHz (minimum supported speed is 133 MHz).
  - A maximum of four processors per computer is supported. Processors from the Intel Pentium/Celeron family, AMD K6/Athlon/Duron family, or compatible processors are recommended.
  - **256 megabytes (MB)** of RAM recommended minimum (128 MB minimum supported; 4 gigabytes (GB) maximum).
  - A hard disk partition or volume with enough free space to accommodate the setup process. To ensure that you have flexibility in your later use of the operating system, it is recommended that you allow considerably more space than the minimum required for running Setup, which is approximately 1.25 GB to 2 GB. partition **(NTFS is the recommended file system).**
  - VGA or higher-resolution monitor (Super VGA 800x600 or higher recommended), keyboard, and
  - **(optionally)** a mouse or other pointing device.

System Partition

- Stores hardware-specific files needed to boot operating system
- Intel-based, the active partition serves as the system partition
- Files found on this partition
  - NTLDR — Windows 2003 boot loader program
  - BOOT.INI — describes the location of the boot partitions, specified by using Advanced RISC Computing (ARC) naming conventions
  - NTDETECT.COM — hardware detection

Boot Partition

- Contains the operating system files
- Default for 2000 is WINNT
- Can have more than one boot partition depending on how many o/s installed
- The BOOT partition & SYSTEM partition can be the same physical partition
- SYSTEM partition contains boot files and BOOT partition contains 2003 system files

Performing an Installation

- **Attended installation**
  - The name of the new server
  - Which network protocols that the Setup Wizard will install
  - Which optional software components that the Setup Wizard will install
  - The date, time, and time zone of the server
  - The product ID number, which is usually printed on a label affixed to the
  - Windows Server 2003 CD-ROM jewel case (assuming you purchased Windows Server 2003 through a retail channel; if you didn’t, see the sidebar, “Activation Keys and Product IDs”).

Cont.

You can begin an attended setup by running the Setup Wizard directly:

- For a CD-based installation, run **winnt32.exe** if the computer is already running a version of Windows. If the computer has been booted using a DOS floppy disk, run **winnt.exe**. Both executables can be found in the **i386** subfolder on the Windows Server 2003 CD-ROM.
- For a network-based installation, run **winnt32.exe** or **winnt.exe** from the network copy of the Windows Server 2003 CD-ROM.
- For a RIS-based installation, start the installation process normally, using your RIS boot floppy or a PXE-compatible NIC. A special Mini Setup Wizard automatically runs after the RIS image has been copied and the computer has been rebooted.

Installation options

When you start the installation process by running **winnt32.exe** or **winnt.exe**,

- For example, to specify the **/dudisable** option, just run **winnt32.exe /dudisable** or **winnt.exe /dudisable**.
- **/checkupgradeonly**.
- **/dudisable**.
- **/makelocalsource.**

Unattended installation

Attended installations can be time-consuming because they require you to physically enter so many pieces of information.

- ***Creating an answer file***

The sample answer file looks something like this:

```
[Unattended]
Unattendmode = FullUnattended
OemPreinstall = NO
TargetPath = *
Filesystem = LeaveAlone
[UserData]
FullName = “Your User Name”
OrgName = “Your Organization Name”
ComputerName = *
ProductKey= “JJWKH-7M9R8-26VM4-FX8CC-GDPD8”
[GuiUnattended]
; Sets the Timezone to the Pacific Northwest
; Sets the Admin Password to NULL
; Turn AutoLogon ON and login once
TimeZone = “004”
AdminPassword = *
AutoLogon = Yes
AutoLogonCount = 1
```

- ***Product Activation***
  - –Microsoft requires all operating system installations to be *activated*

Upgrading from Prior Versions of Windows

- Windows Server 2003 can perform an upgrade if your computer is already running:
  - Windows NT Server 3.51,
  - Windows NT Server 4.0, or
  - Windows 2000 Server
- cannot perform an upgrade on a computer running:
  - Windows 9x,
  - Windows NT Workstation, or
  - Windows 2000 Professional.

Product Activation

- Product activation is tied to the product ID number you provide to the Setup Wizard when you install Windows Server 2003.
- Product Activation Compared to Product Registration
  - product activation is required
  - Product registration is completely optional
    - All registration information provided is stored securely

What licensing mode to use

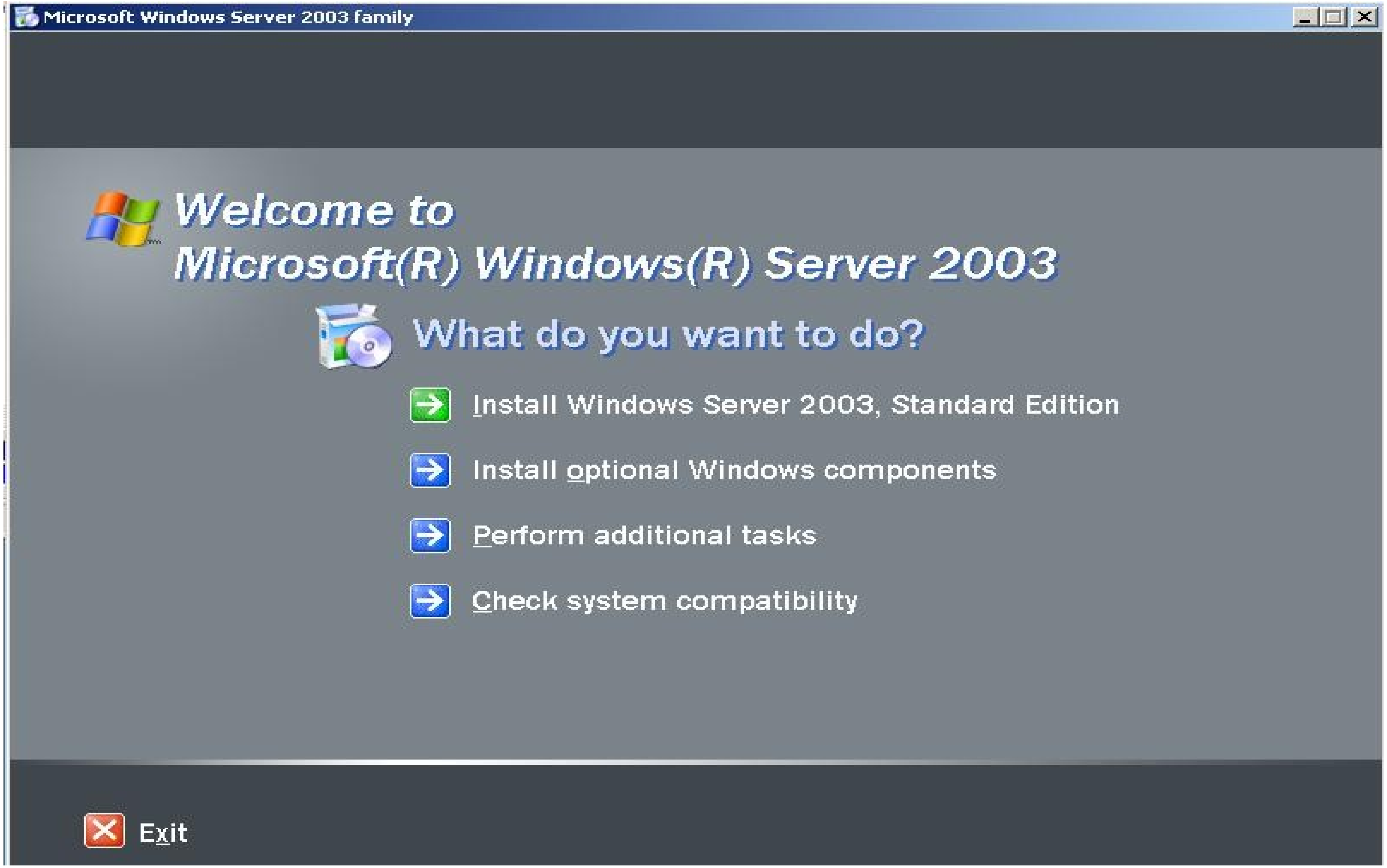
With products in the Windows Server 2003 family, you can choose between two licensing modes:

- **Per Device or Per User**
  - Per Device or Per User mode requires a separate Client Access License (CAL) for each device or user that accesses a server running a product in the Windows Server 2003 family.
  - Per Seat/User more economical for large organizations
    - This is what USMC uses. Each Computer connecting has a license
- **Per Server**
  - Per Server mode requires a separate CAL for each concurrent connection to a server.

Headless Servers

- Many companies prefer to keep their servers in secure, environmentally controlled data centers
  - There is really very little need for them to have keyboards, monitors, or mice.
- Certain key functions of a server do require a monitor, keyboard, and mouse.
  - working with the computer's built-in BIOS configuration usually must be done from the *console,* or the server's physical keyboard.
- Windows Server 2003 supports CD-based, network-based, and RIS-based installations on headless servers.
  - Headless server installations can be performed only on server hardware that is compatible with Windows Server 2003's headless server capabilities

Setup Menu



Microsoft Windows Server 2003 family

Welcome to
Microsoft(R) Windows(R) Server 2003

What do you want to do?

- Install Windows Server 2003, Standard Edition
- Install optional Windows components
- Perform additional tasks
- Check system compatibility

Exit

REVIEW

In this session, you learned about the various installation methods supported by

- Windows Server 2003:
- CD-based
- Network-based
- RIS-based

You also learned about attended and unattended installations, how to create
answer files for unattended installations, and how to start both attended and
unattended installations. You learned about Windows Server 2003's ability to
upgrade your computers' existing operating systems, and you learned about the
product activation required by Windows Server 2003. Finally, you learned about
Windows Server 2003's new "headless server" installation capabilities.

QUIZ YOURSELF

1. What are the three ways you can install Windows Server 2003?

2. How do you initiate a CD-based installation? (See “CD-based installation.”)

3. What two commands can be used to initiate a network-based installation?

4. What special type of network interface card (NIC) is required to perform an installation using RIS?

5. What are two ways to create an answer file for use in an unattended installation?

6. What operating systems can be upgraded to Windows Server 2003?

Using Active Directory

- Why Use Active Directory?
- How Active Directory Works
  - Domain requirements
  - Domain Structure
- Planning a Domain
  - Laying out domains
    - Single domains
    - Domains trees
    - Forests
  - Deciding on OU’s
- Making a Domain Controller
- Managing Domain Users and Groups
- Review
- Quiz Yourself

Using Active Directory

- How to design an Active Directory domain
- How to promote a server to be a domain controller
- How to manage domain users and groups

Why Use Active Directory?

Standalone and member servers

- You have to create user accounts on each server when someone joins your organization and remove those accounts when someone leaves.
- Users have to provide a user name and password each time someone accesses resources on a different server.
- When it’s time to change users’ passwords, users must do so on each server.

Active Directory provides a central list of users and groups, which is called a *domain.*

- You only have to create user accounts once—in the domain.
- Users only provide their user names and passwords once—when they log on to the domain.
- When they change their passwords, users only do so once—in the domain.

How Active Directory Works

- Active Directory is built around special servers called domain controllers, or DCs.
- DCs all contain a copy of the domain database, which is often referred to simply as “the directory.”
  - The directory contains all of the domain user and group accounts, as well as configuration information about the domain itself.
- All of the DCs in a domain use a process called *replication* to ensure that each DC has the same domain information as the others.
- Users simply provide their domain user name and password, and the workstation communicates with a DC to make sure the user name and password match.

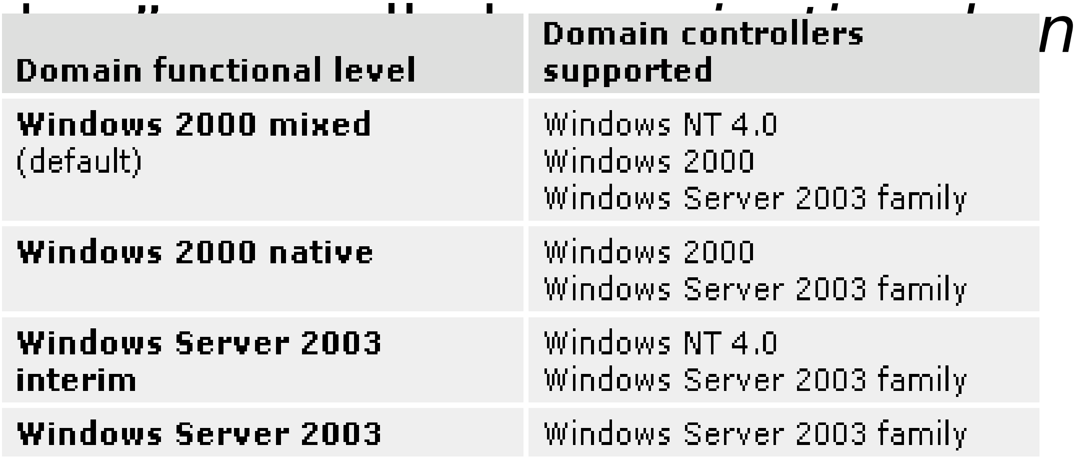
Domain requirements

- Active Directory DCs must be running Windows 2000 Server, Windows Server 2003, or a later version of the Windows Server operating system. Active Directory also requires a Domain Name Service (DNS) server, although you can install and run a DNS server on one or more of your DCs, if necessary.

- Your DNS server must also support two special features:
  - SRV records, which allow a DNS server to keep track of network servers that offer special functionality, like Active Directory domain controllers
  - Dynamic updates, which allow computers to insert their name information into a DNS server automatically, rather than requiring an administrator to manually update the DNS database

Domain structure

- A domain is really nothing more than a special kind of database, and all databases have a structure.
  - The structure is hierarchical, or tree-like, much like the “tree” of folders on your computer’s hard drive.
- The domain itself is the “root” of the tree. The “branc *nits,* or OUs.



Domain functional level	Domain controllers supported
Windows 2000 mixed (default)	Windows NT 4.0 Windows 2000 Windows Server 2003 family
Windows 2000 native	Windows 2000 Windows Server 2003 family
Windows Server 2003 interim	Windows NT 4.0 Windows Server 2003 family
Windows Server 2003	Windows Server 2003 family

Domain

- Logical grouping of computers and users
- Share a central directory database w/security and user account information
- Managed by at least one 2003 Server domain controller (DC)
  - DCs manage all security-related user/domain interactions and centralizes administration
  - All computers in domain w/access to database
  - 2003 Servers configured as either DCs or stand-alone servers
  - Only peer domain controllers -- no PDC

Domain

- Core unit of replication, security and logical structure in 2003
- Possibly contain up to 10+ million objects
- As a security boundary, security policies do not cross from one domain to another
- Domains contain W2K3 domain controllers, W2K3 member servers or 2000 Professional computers

Domain Advantages

- Provides centralized administration
- Provides a single logon process
- Provides scalability to create large networks
- Disadvantages?

Planning User Accounts

- Naming conventions must be consistent and uniquely identify users to the domain
- Use unique logon, max of 20 characters
- Logon names are not case sensitive
- Invalid characters – / \ [ ] : ; | = , + * ? < >
- Name space designations appended to logon
  - SMITHCA = smithjj@mstp.quantico.usmc.mil
- Passwords assigned, hard to guess and no longer than 128 characters (8 recommended)
  - Passwords can contain spaces, a good method for creating passwords is to use a phrase or sentence "I love Windows 2000 server"

Trusts in Windows 2003

- Two-way trust – A trust relationship between two domains in which both domains trust each other; domain A trusts domain B, and domain B trusts domain A
- Transitive trust -- A trust that flows throughout a set of domains; if domain A has a transitive trust with domain B, and domain B trusts domain C, then domain A trusts domain C.
- When a child domain joins the domain tree it immediately has trust relationships with every domain in tree
- For interaction between multiple domains, trust relationships are necessary

Planning a Domain

- Who will manage the user and group accounts?
- What users share common security and configuration requirements?

Laying out domains

- Smaller organizations can usually use a single domain because all of their users and groups are managed by a single group of individuals.

Single domains

- The easiest configuration is a single domain.

Domain trees

- Large organizations usually distribute the management of their user and group accounts. In those distributed situations, a domain tree with parent and child domains is often appropriate.

Making a Domain Controller

- To create a domain controller, install Windows Server 2003 on a computer. Then, open the Start menu and select Run.
  - Type **dcpromo.exe** and click OK.
- The Domain Controller Promotion Wizard walks you through the process of promoting the server to be a domain controller.

How Many DCs Do You Need?

- Every domain (both root and child domains) should contain at least two domain controllers, to ensure that the domain continues running even if one server fails.

Managing Domain Users and Groups

The built-in groups include:

Domain Administrators. This domain group has full control over the domain. This group is similar to the local Administrators group included on each server.

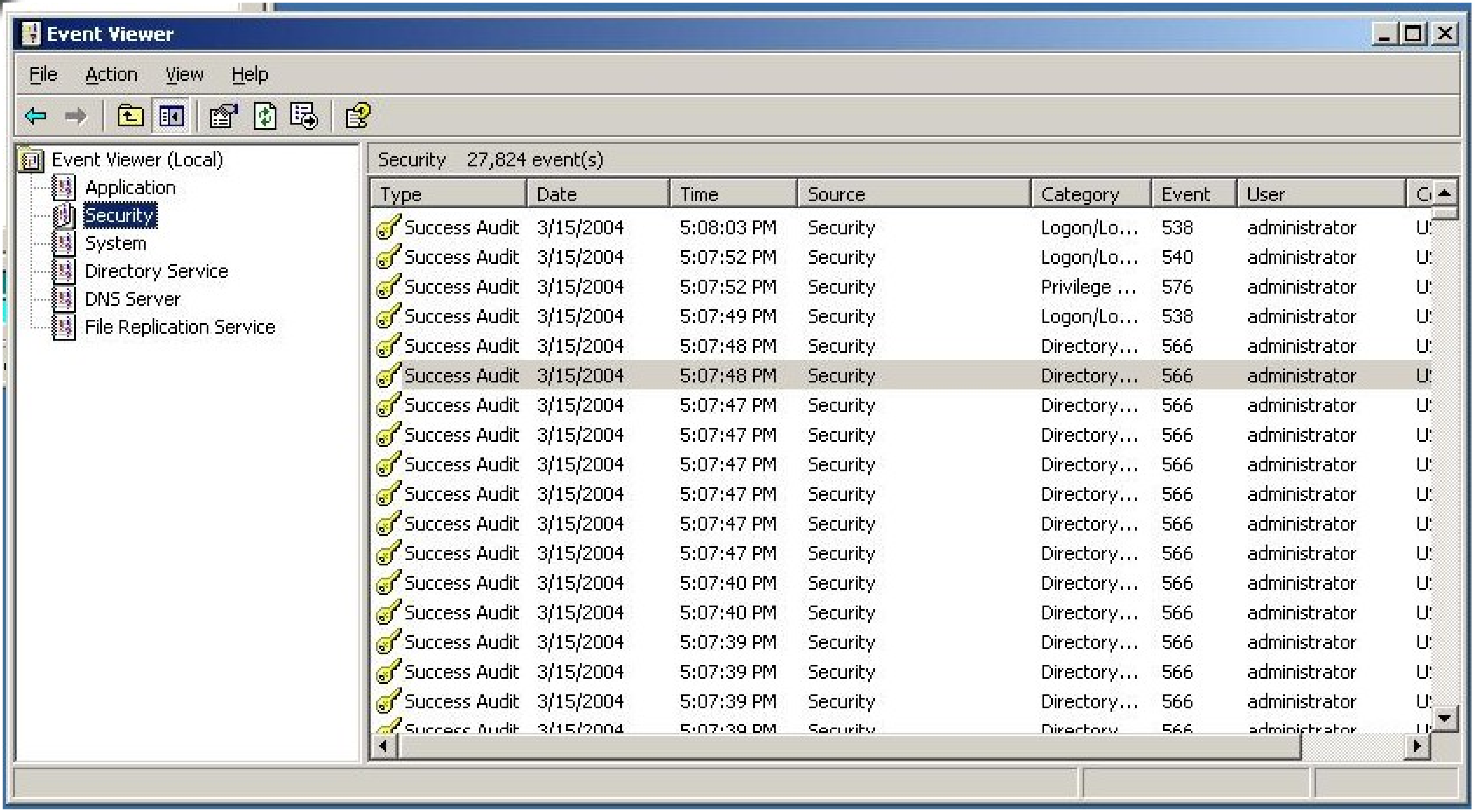
Enterprise Administrators. This domain group has full control over an entire forest.

The types of groups used within Active Directory are:

Domain local groups. These groups can be used only by members of a domain and can contain domain user accounts and domain global groups. For example, you generally assign file and folder permissions to domain local groups.

Domain global groups. These groups can be used by all domains within a tree and can contain only domain user accounts. **Universal groups.** These groups can be seen by all members of a forest. These groups are used only occasionally and can contain users and other universal groups.

Active Directory Users and Computers



Security 27,824 event(s)

Type	Date	Time	Source	Category	Event	User	C
Success Audit	3/15/2004	5:08:03 PM	Security	Logon/Lo...	538	administrator	U
Success Audit	3/15/2004	5:07:52 PM	Security	Logon/Lo...	540	administrator	U
Success Audit	3/15/2004	5:07:52 PM	Security	Privilege ...	576	administrator	U
Success Audit	3/15/2004	5:07:49 PM	Security	Logon/Lo...	538	administrator	U
Success Audit	3/15/2004	5:07:48 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:48 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:40 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:40 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:39 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:39 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:39 PM	Security	Directory...	566	administrator	U
Success Audit	3/15/2004	5:07:39 PM	Security	Directory...	566	administrator	U

REVIEW

You learned how Active Directory can be a useful addition to your network, and how it can save time and headaches for both yourself and your users. You learned the basics of how Active Directory works, and how to plan an Active Directory domain. You also learned how to promote a server to be a domain controller, and how to manage the users and groups in a domain.

QUIZ YOURSELF

MSTP

1. Why would you want to use Active Directory?

2. What process allows domain controllers to synchronize their copies of the directory?

3. How do you change a member server to a domain controller, or vice-versa?

4. Several top-level domains that trust one another form a what?

5. What application is used to manage Active Directory users and groups?

File and Partition Sizes

- NTFS can store up to 16 exabytes in size.
  - Exabyte =1,000,000GB   -Terabyte =1,000GB
- Minimum partition size for NTFS is 50MB.
- Anything smaller – FAT recommended
- NTFS takes nearly 25% of the partition’s total space for directory overhead, whereas FAT takes almost none.
- You can reclaim the space taken by NTFS by setting compression on the entire volume, this is not available on FAT.

NTFS Fault Tolerance

- NTFS logs all changes to the file system, which means it can redo or undo every file or directory update to correct discrepancies arising from system failures or power losses.
- Uses a method called *hot fixing* repair disk failures on the fly; hot fixing does not return an error message to the calling application.
- After every write to a hard disk, the sector is reread to verify it’s integrity.
  - *If data is different, the sector is flagged bad and the write is preformed again to a different place.*

INSTALL PHASES

Install Phases

- Pre-Copy Phase
  - files copied into temp directory
- Text Mode
  - Licensing, existing installs, install partition, install file system, 2003 files location
- Gathering Information
  - Regional Settings, Name and Organization, License Mode**,** Computer Name, Password, Optional Components, Date and Time

Install Phases

- Networking
  - Install detected network adapters, Typical (uses DHCP) or Custom settings, IIS installed
- Completing Setup
  - Copying files, configuring the computer, save configuration, removes temp files, reboot

CONFIGURATION

AD RECAP

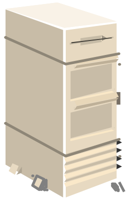
- Designing domain structure to meet needs and structure of organization
- Include directories of information about network resources and services
- Simplified administration
- Organizes resources in a hierarchical structure

AD RECAP CONT.

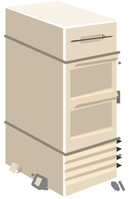
- Collection of info uniquely identifying users and resources on a network
- Provides organization and access to users and resources
- Allows for the enforcement of security to protect objects
- Replicates the directory to other computers automatically for fault tolerance
- Allows partitioning of the directory for storage of large numbers of objects

AD RECAP CONT.

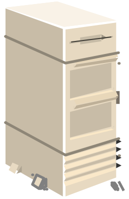
- Users typically work with multiple shares on a daily basis
- Share names often have little to do with share *functions*
- Mapped drives are common
  - P: → \\Minerva\Rpts
  - H: → \\B2F2S2\Users
- Drive mappings are group and machine dependent
  - (Marketing) H: →\\NYFin2\Public
  - (Development) H: → \\B2F2S2\Users
- Physical names lead to higher TCO and downtime



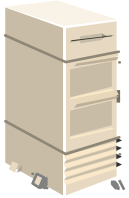
\\Minerva\Rpts



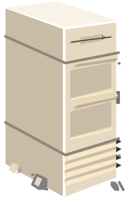
\\NYFin2\Public



\\B2F2S2\Users



\\Hercules\Status

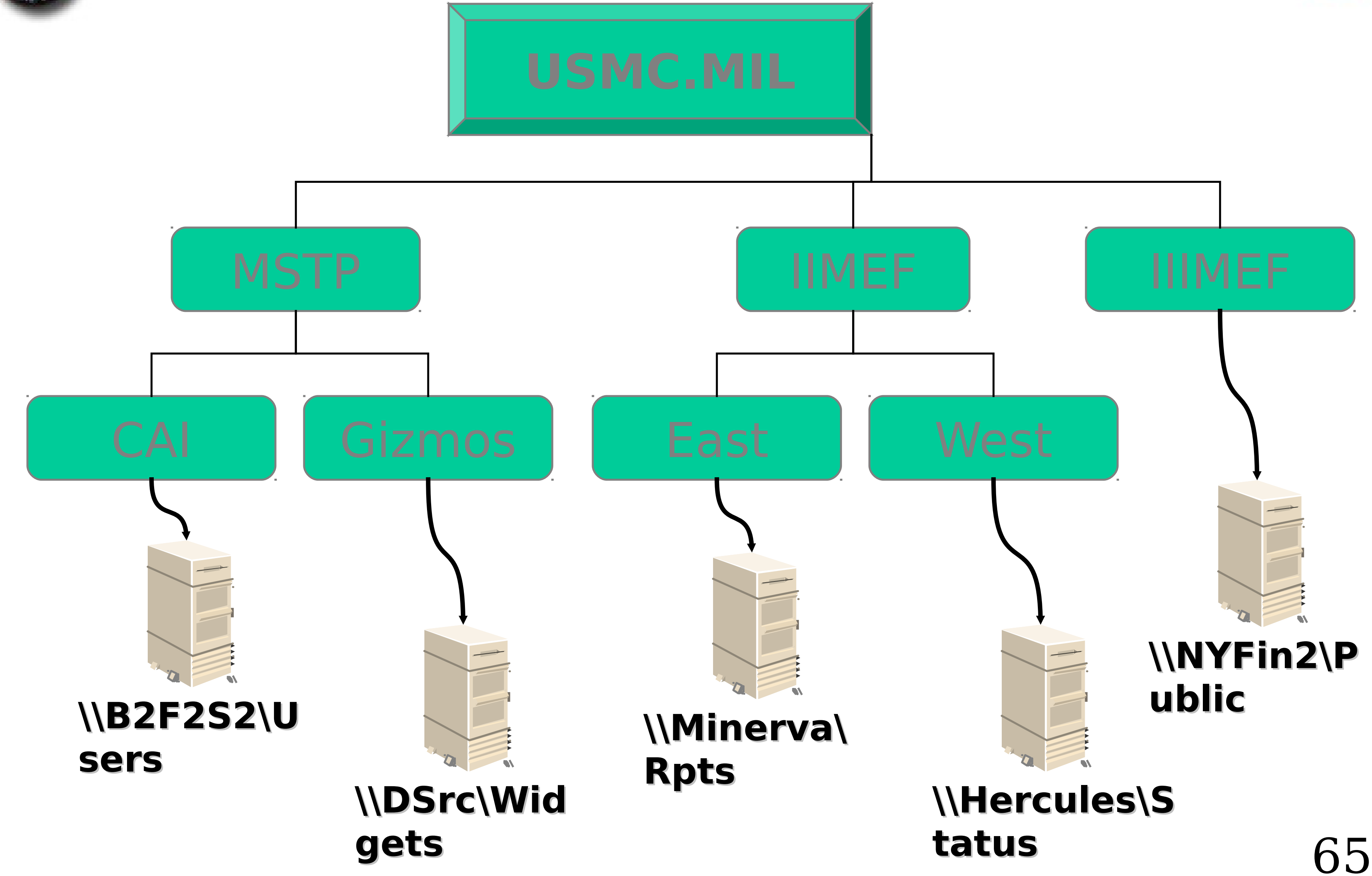


\\DSrc\Widgets

AD RECAP CONT.

- A logical namespace solves many of these problems
  - Shares can be assigned names that more closely match function
  - Multiple machines can be mapped to single logical names
  - Single drive mapping can accommodate the entire namespace
  - Simplify and hide the physical topology
  - Consistent, global naming for users

AD RECAP CONT.



Domain Controller Setup

- No need to promote or demote a domain controller
- Add additional domain controllers for redundancy and reduce the load on existing domain controllers
- To install 2003 Server execute command **dcpromo**
- If create first DC in domain, creating either a new child domain, or new domain tree

Network Setup

- If this is the first computer in the domain network setup will have to wait until your services are configured
- Joining an existing domain as a member server is the same as joining an NT domain

DCPROMO

- Makes 2003 Server a domain controller
- Run after reboot server installation
  - O/S is 2003 Server, Standard Edition or Enterprise
  - TCP/IP must be installed
  - Network connectivity must exist
  - The correct time and zone must be specified
  - DNS server available on the network
    - If not, DCPROMO will create this server as one
  - One NTFS volume is required for Active Directory
  - User with administrative rights

WINDOWS 2003 LAB

- DCPROMO LAB

WINDOWS 2003 LAB

- Sites and Subnets
  - Creating sites and assigning subnets to those sites

WINDOWS 2003 LAB

- ADI DNS
  - Integrate DNS into AD

USER MANAGEMENT

Managing Users and Groups

- Server Security
- Local Users and Groups
  - Users
    - Managing users
    - Built-in users
  - Groups
    - What groups should you create
    - Managing groups
    - Built-in groups
- Local Account Policies
  - Password polices
  - Account Lockout policies
- Security Auditing
- Review
- Quiz Yourself

Managing Users and Groups

- How to add local users and groups
- How server security works
- How to configure local account policies
- How to configure security auditing

Workgroup

- Logical grouping of computers and users that share resources
- Each 2003 computer maintains a local directory database with its own accounts, administration, and security policies
- Similar to a peer-to-peer network
- Decentralized management
- Resources password protected, but must know
- Professional workstation or stand-alone server

Workgroup Advantages

- Does not require a central server for administration
- Simple to design and implement
- Convenient for a limited number of computers, normally 10 or less
- Good for small amount of technical users
- Disadvantages?

Server Security

Windows Server 2003 can play different roles on a network, depending on your security requirements:

- As a ***standalone server***, Windows Server 2003 maintains its own user accounts and groups.
- As a ***domain controller***, Windows Server 2003 maintains user accounts and groups that can be shared with other servers.
- As a ***member server***, Windows Server 2003 maintains its own user accounts, just like a standalone server.

Local Users and Groups

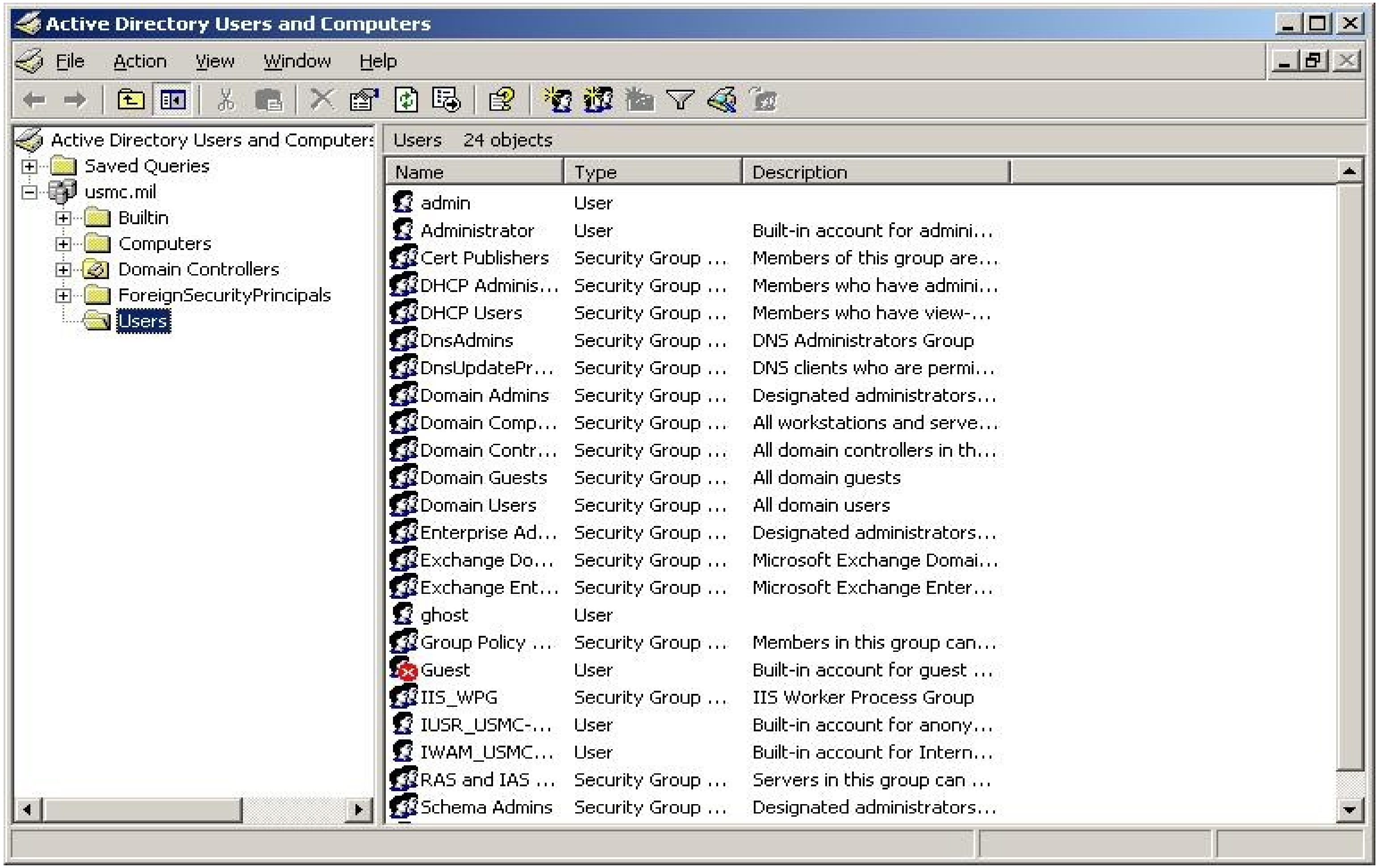
A *user*, or *user account,* represents a real person who needs to use the resources on a server.

- ***Users***
  - User accounts are configured with several pieces of information:
    - A user name, or user ID, which uniquely represents and identifies the account—for example, “JoeL,” “Djonw,” or “RrondA.”
    - A proper name, which is the user’s full name.
    - A password, which is a series of numbers, symbols, and letters.
    - Account properties, which define special information about the user.

Cont.

- ***Managing users***
  - Windows Server 2003 enables you to create user accounts using the Computer Management application
  - The application is located in the **Administrative Tools** folder, which can be accessed from the Start menu.

Cont. Managing users and groups with the Computer Management application

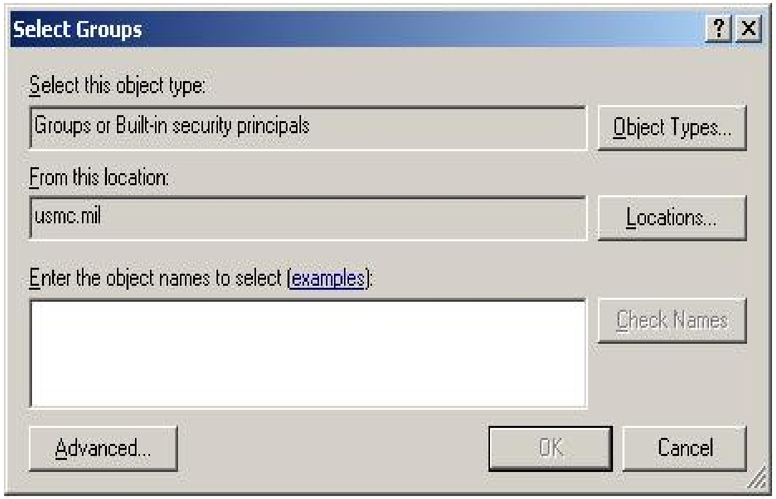

Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers
Saved Queries
usmc.mil
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

Users 24 objects

Name	Type	Description
admin	User	
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Exchange Do...	Security Group ...	Microsoft Exchange Domai...
Exchange Ent...	Security Group ...	Microsoft Exchange Enter...
ghost	User	
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_USMC-...	User	Built-in account for anony...
IWAM_USMC...	User	Built-in account for Intern...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...

- Changing users’ passwords when they forget them
- Locking and unlocking user accounts to control access to the server
- Creating new user accounts and deleting old ones

Cont.


Select Groups

Select this object type:
Groups or Built-in security principals

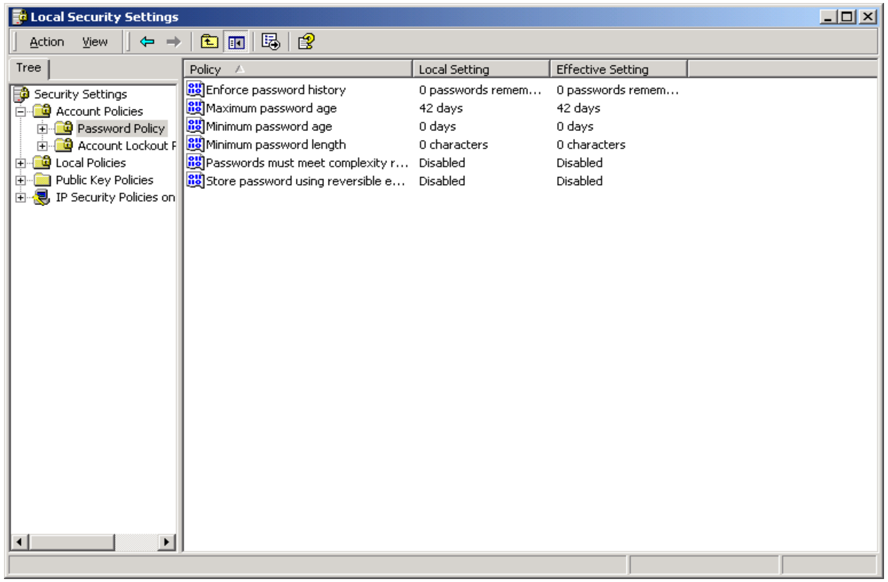
From this location:
usmc.mil

Enter the object names to select (examples):

Built-in groups

Administrators. Members of this group can perform any action on the server.
Server Operators. Members of this group can perform tasks such as shutting
the server down, controlling access to files and folders, and so forth.
Print Operators. Members of this group can manage the printers that may
be attached to a server.
Backup Operators. Members of this group are allowed to read any file or folder on the server, for the purpose of copying those files and folders to backup tapes.

Local Account Policies



Policy	Local Setting	Effective Setting
Enforce password history	0 passwords remem...	0 passwords remem...
Maximum password age	42 days	42 days
Minimum password age	0 days	0 days
Minimum password length	0 characters	0 characters
Passwords must meet complexity r...	Disabled	Disabled
Store password using reversible e...	Disabled	Disabled

Managing local account policies

Password policies

Password policies control how your users' passwords are treated.

Enforce password history. This policy tells Windows Server 2003 to remember the passwords your users have used in the past.

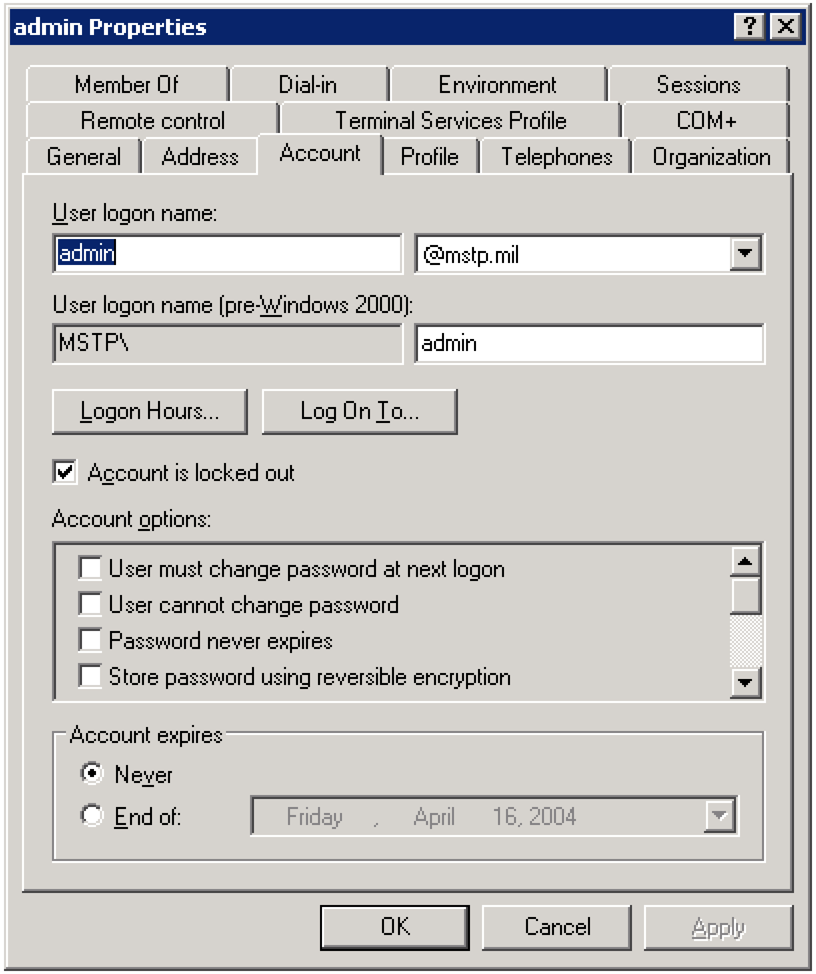
Maximum password age. You can configure the maximum number of days that users can keep their passwords.

Minimum password age. You can configure the number of days users must wait before changing their passwords again.

Minimum password length. Short passwords are easy for hackers to guess.

Cont.

- ***Account Lockout policies***
  - **Account lockout threshold.** This policy determines how many times Windows Server 2003 enables someone to try to access a user account with the wrong password.
  - **Account lockout duration.** This policy determines how long an account remains locked out.



User logon name: admin @mstp.mil

User logon name (pre-Windows 2000): MSTP\ admin

☑ Account is locked out

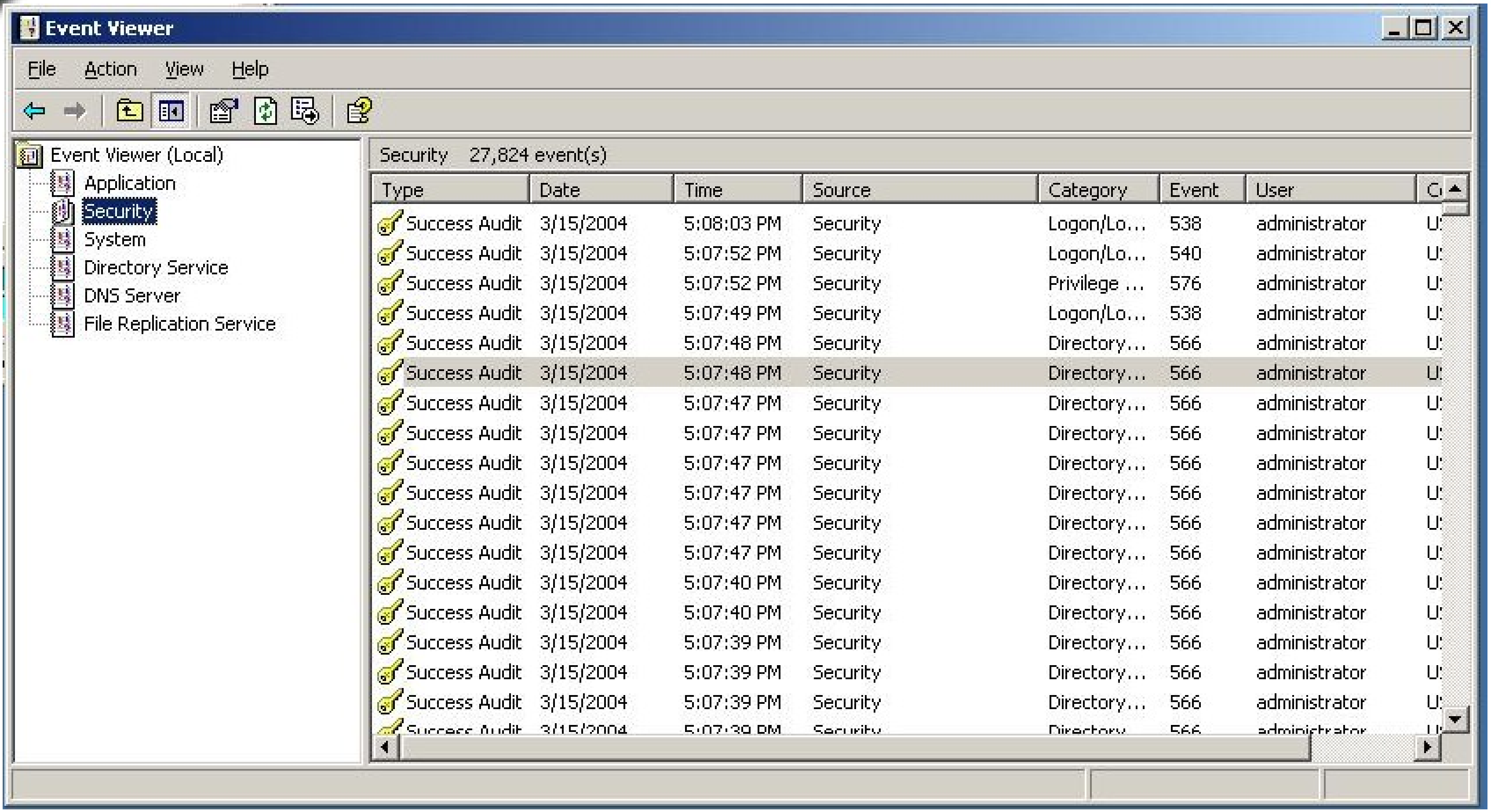
Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Friday , April 16, 2004

Security Auditing



Event Viewer (Local)
- Application
- Security
- System
- Directory Service
- DNS Server
- File Replication Service

Security 27,824 event(s)

Type	Date	Time	Source	Category	Event	User	C
Success Audit	3/15/2004	5:08:03 PM	Security	Logon/Lo...	538	administrator	U:
Success Audit	3/15/2004	5:07:52 PM	Security	Logon/Lo...	540	administrator	U:
Success Audit	3/15/2004	5:07:52 PM	Security	Privilege ...	576	administrator	U:
Success Audit	3/15/2004	5:07:49 PM	Security	Logon/Lo...	538	administrator	U:
Success Audit	3/15/2004	5:07:48 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:48 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:47 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:40 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:40 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:39 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:39 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:39 PM	Security	Directory...	566	administrator	U:
Success Audit	3/15/2004	5:07:39 PM	Security	Directory...	566	administrator	U

Cont.

The Audit policies include:

- **Audit logon events.** This policy tells Windows Server 2003 to create Security Event Log entries whenever someone attempts to access the server.
- **Audit account management.** This policy audits the creation, modification, or deletion of user and group accounts.
- **Audit object access.** This policy allows Windows Server 2003 to audit file and folder access, helping to keep track of what files and folders are being accessed by users.
- **Audit policy change.** This policy audits any changes to the local security policies, so you can see if another user has changed the policies you have defined.

Old Server Manager Tasks

- Shared Folders snap-in via an MMC
  - Remote management of shared folders
  - Remote viewing of which users are accessing shared resources
  - Remote disconnection of users from shared resources on a 2003 computer
  - Send a message
- Services snap-in via an MMC
  - Remote starting and stopping of services
- Specify remote computer when creating custom MMC

Old Server Manager Tasks

- Add/remove computer from domain
  - During installation of 2003 O/S
  - To join domain, computer account must be created in or added to domain either during install or in advance (AD Users & Computers)
    - Users w/ Join A Computer to the Domain user right
    - Members of Administrators, Domain Administrators, or Account Operators
  - DC & DNS must be online when installing
- Join domain by using Network Identification tab in System Properties

Creating Domain User Accounts

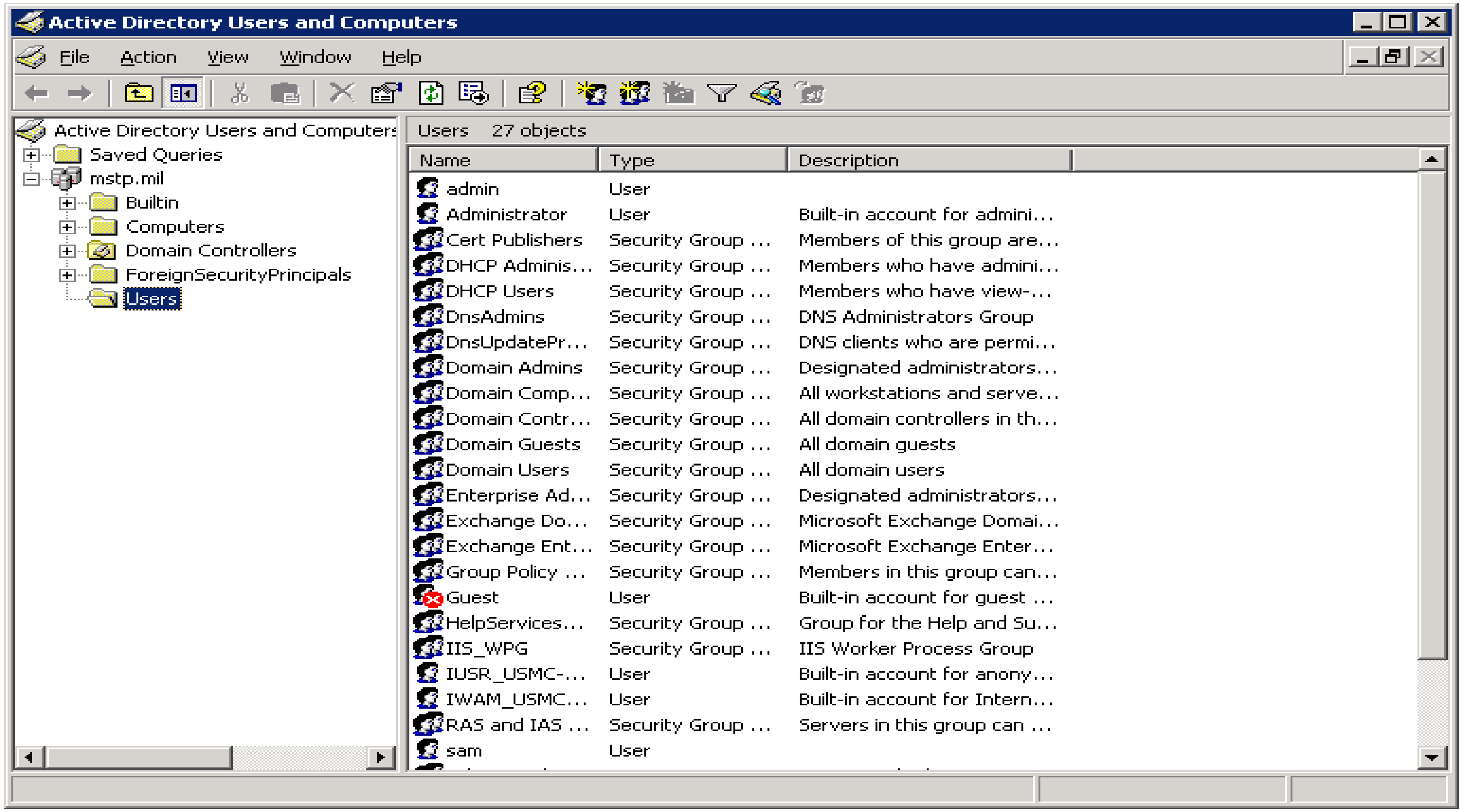
- Use MMC with Active Directory Users and Computers
- From the Domain Controller Start/Programs/Administrative Tools/ACTIVE DIRECTORY USERS AND COMPUTERS

WINDOWS 2003 LAB

- MMC Creation
  - Create a custom MMC using common snap-ins
  - Create users and groups using ADUG

Creating the User Account

- Select the USERS container (or an OU you may have created)

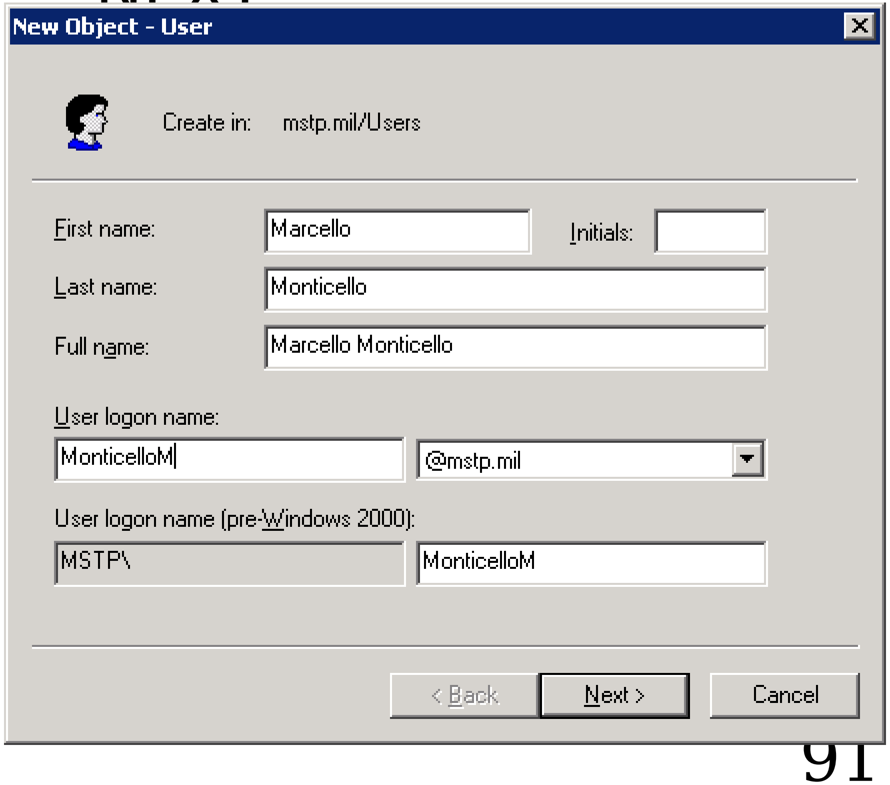


Name	Type	Description
admin	User	
Administrator	User	Built-in account for admini...
Cert Publishers	Security Group ...	Members of this group are...
DHCP Adminis...	Security Group ...	Members who have admini...
DHCP Users	Security Group ...	Members who have view-...
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdatePr...	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Exchange Do...	Security Group ...	Microsoft Exchange Domai...
Exchange Ent...	Security Group ...	Microsoft Exchange Enter...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_USMC-...	User	Built-in account for anony...
IWAM_USMC...	User	Built-in account for Intern...
RAS and IAS ...	Security Group ...	Servers in this group can ...
sam	User	

Creating the User Account

- Action menu select New and Users
- <u>First name</u>: mandatory
- <u>Last name</u>: mandatory
- <u>Full Name</u>: Completed automatically; displayed in OU where acct located
- <u>User Logon Name</u>: Unique based on naming conventions (required)
- Can create accounts in any domain w/permissions

- <u>User logon name (pre-Windows 2000)</u>: Unique name used from NT 4.0 or 3.51 required Click NEXT


New Object - User

Create in: mstp.mil/Users

First name: Marcello

Initials:

Last name: Monticello

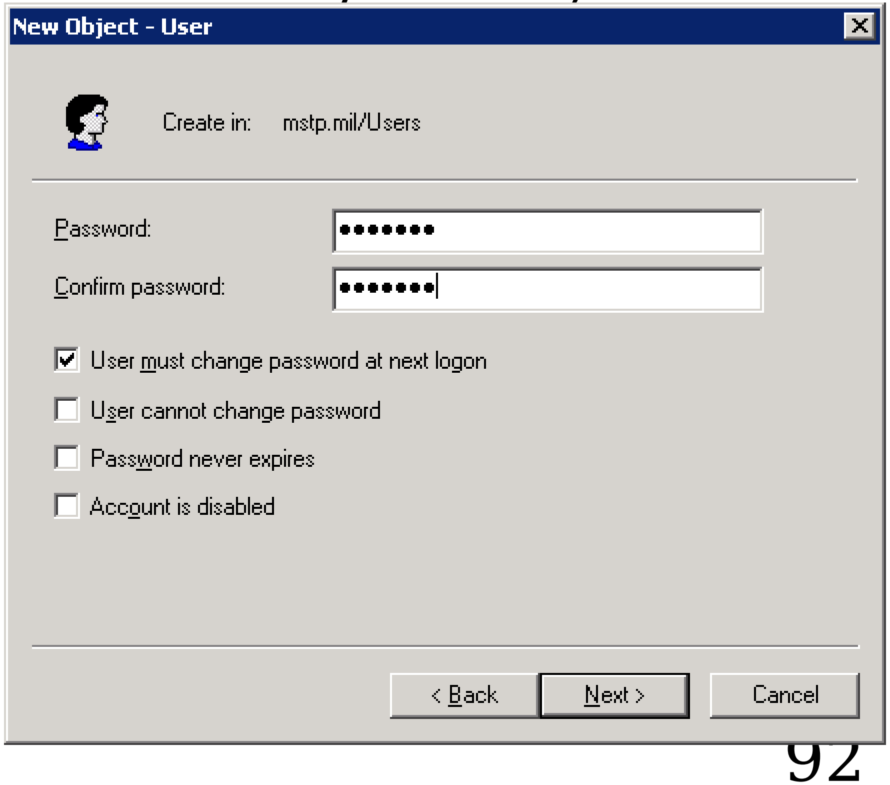
Full name: Marcello Monticello

User logon name: MonticelloM @mstp.mil

User logon name (pre-Windows 2000): MSTP\ MonticelloM

Password Dialog Box

- Password Settings Screen
- Enter initial password and for verification
- Passwords are CASE SENSITIVE
- No check boxes are checked by default
  - User Must Change Password at Next Logon
  - User Cannot Change Password
  - Password Never Expires
  - Account Disabled (Guest account by default)



Create in: mstp.mil/Users

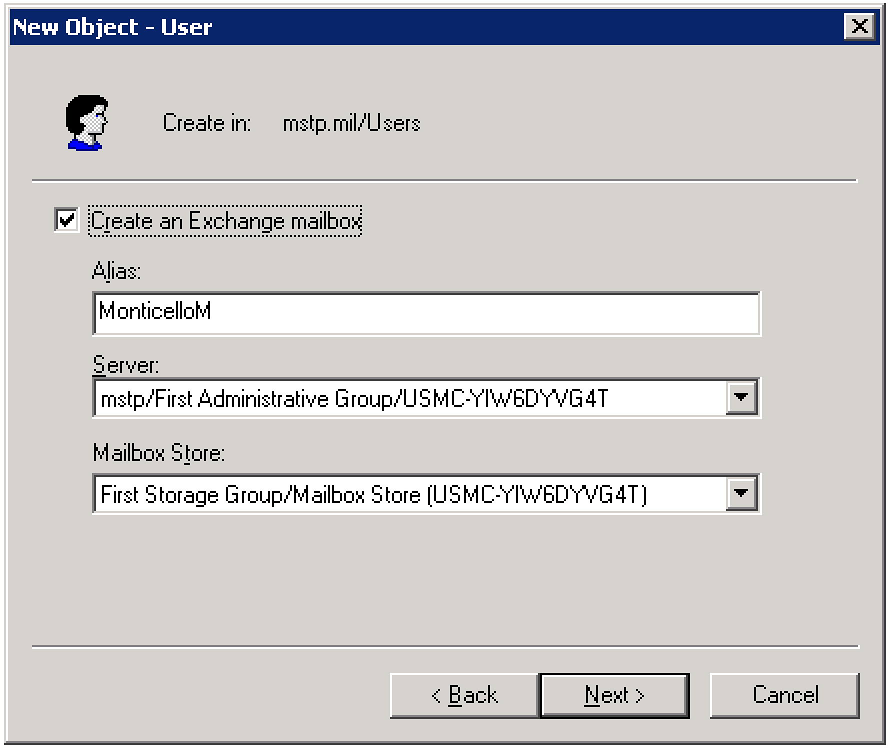
Password: ••••••••

Confirm password: ••••••••

☑ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled

User Finish Screen

- Reviews options selected
- Click Back for changes
- Click Finish if complete



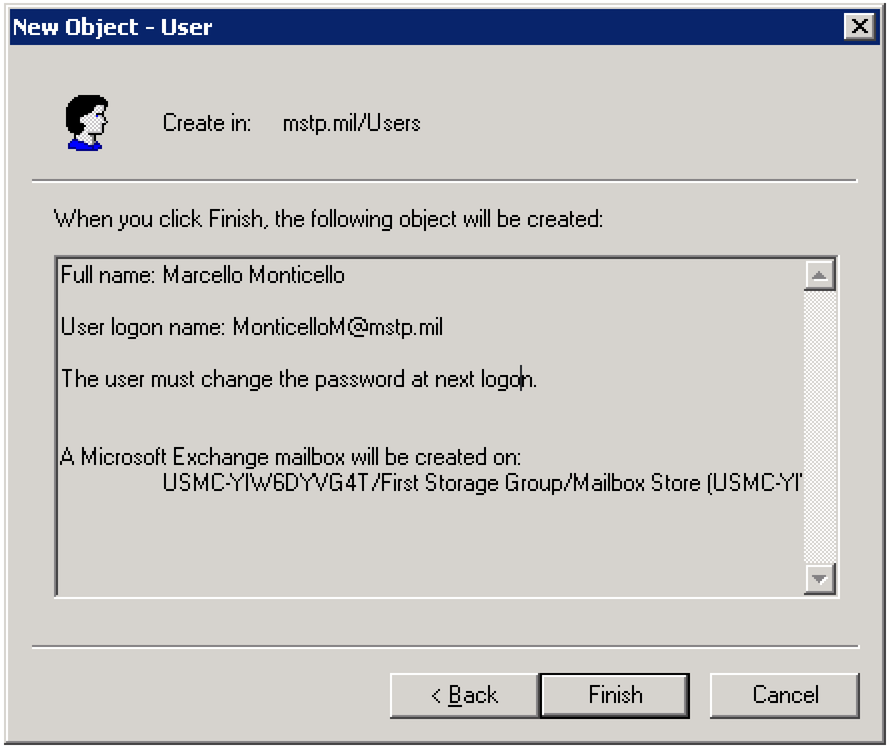
Create in: mstp.mil/Users

☑ Create an Exchange mailbox

Alias: MonticelloM

Server: mstp/First Administrative Group/USMC-YIW6DYVG4T

Mailbox Store: First Storage Group/Mailbox Store (USMC-YIW6DYVG4T)



Create in: mstp.mil/Users

When you click Finish, the following object will be created:

Full name: Marcello Monticello

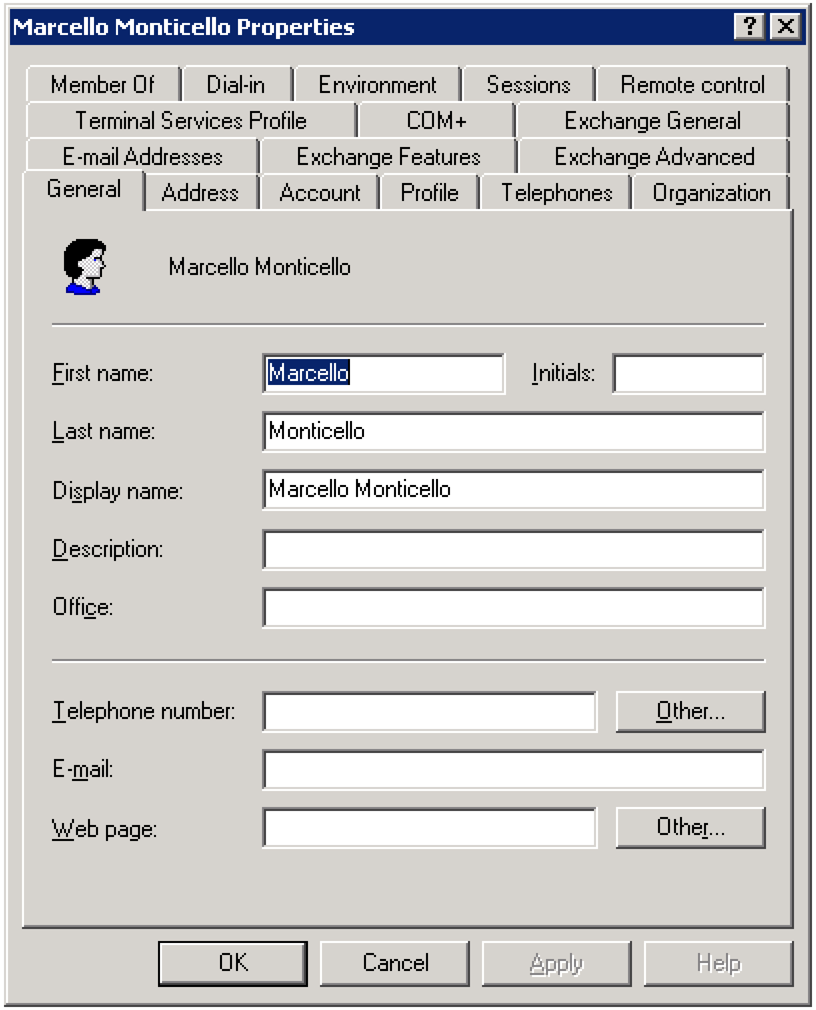
User logon name: MonticelloM@mstp.mil

The user must change the password at next logon.

A Microsoft Exchange mailbox will be created on:
USMC-YIW6DYVG4T/First Storage Group/Mailbox Store (USMC-YI

User General Tab

- Use AD Users and Computers & double-click user object
- Personal properties tab
- Can search info to find users in AD
- Info -- name, description, office location, telephone, e-mail name, & web page



Marcello Monticello

First name: Marcello

Initials:

Last name: Monticello

Display name: Marcello Monticello

Description:

Office:

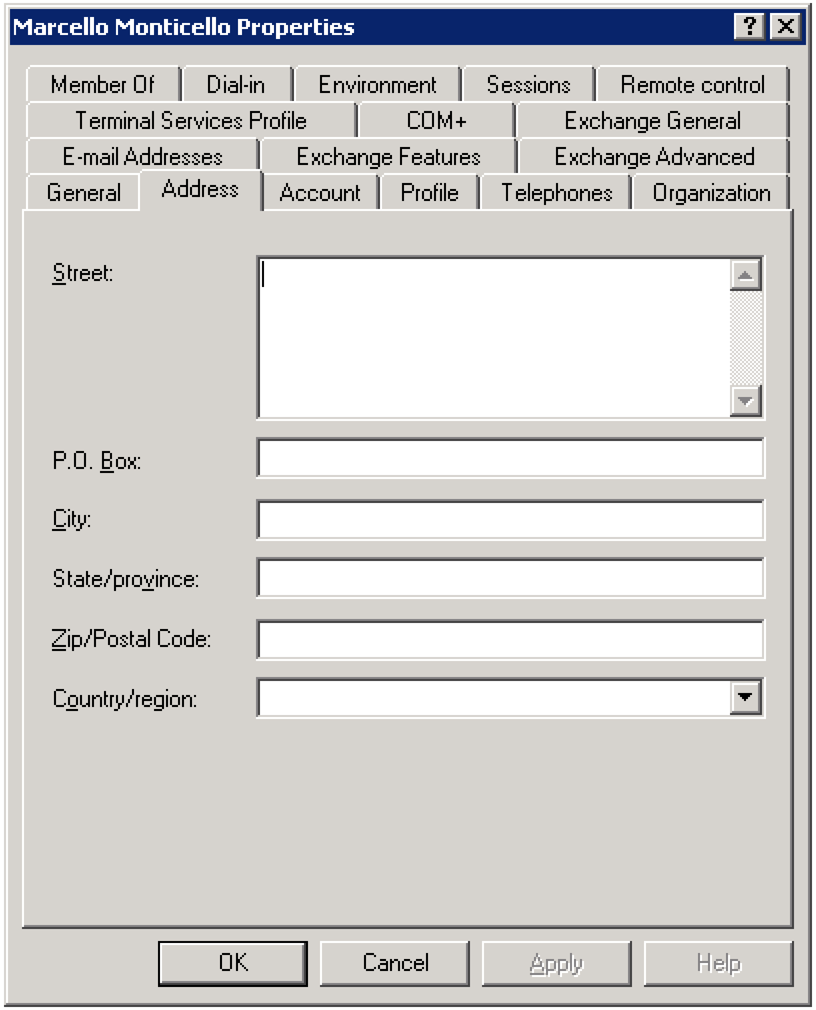
Telephone number:

E-mail:

Web page:

Address Tab

- Personal properties tab
- Records street address, post office box, city, state or province, zip code and country



Street:

P.O. Box:

City:

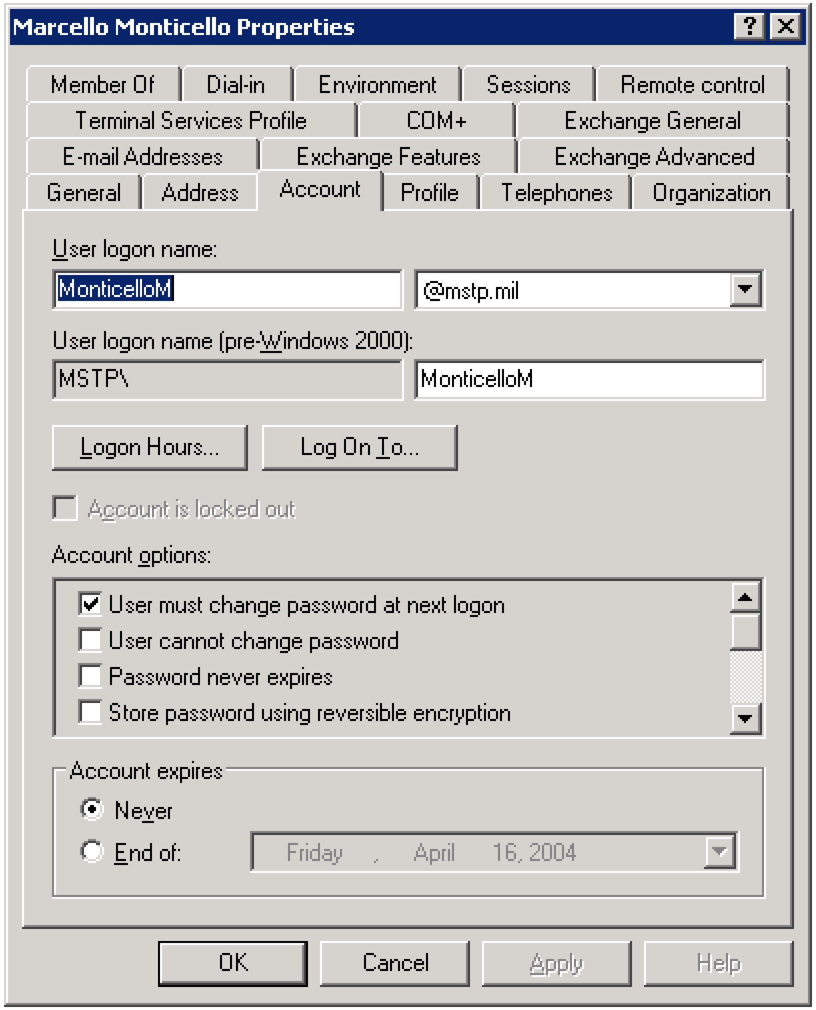
State/province:

Zip/Postal Code:

Country/region:

Account Tab

- Defines logon name and set other account options (some w/defaults)
- **Account** specifies account expiration



Marcello Monticello Properties

User logon name: MonticelloM @mstp.mil

User logon name (pre-Windows 2000): MSTP\ MonticelloM

□ Account is locked out

Account options:

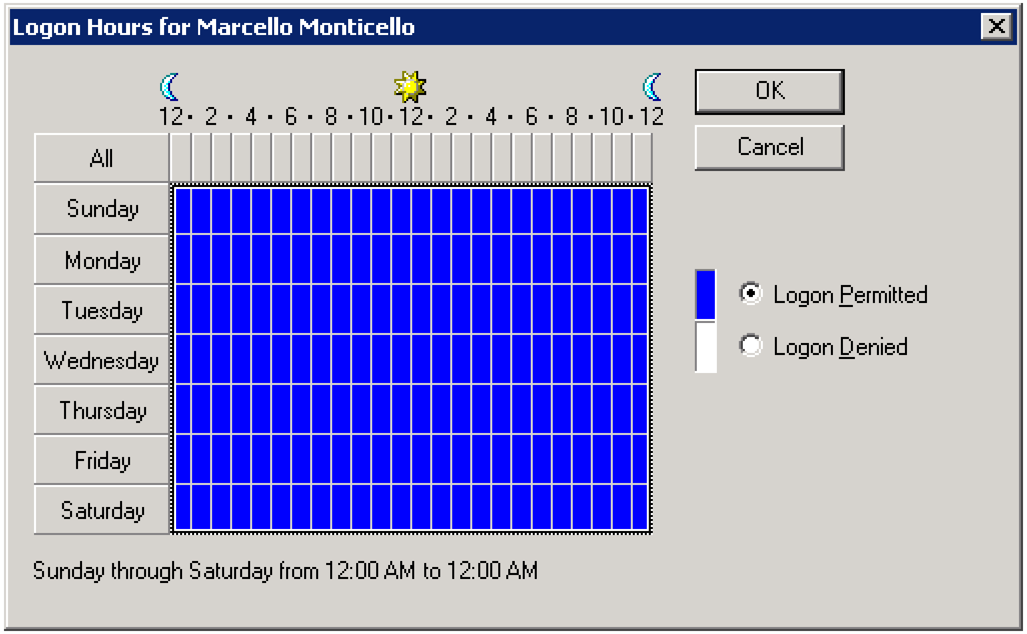
- ☑ User must change password at next logon
- □ User cannot change password
- □ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Friday , April 16, 2004

Account Tab -- Hours

- **Logon Hours** allowed to be logged in
- Highlight Time will be displayed at bottom



Logon Hours for Marcello Monticello

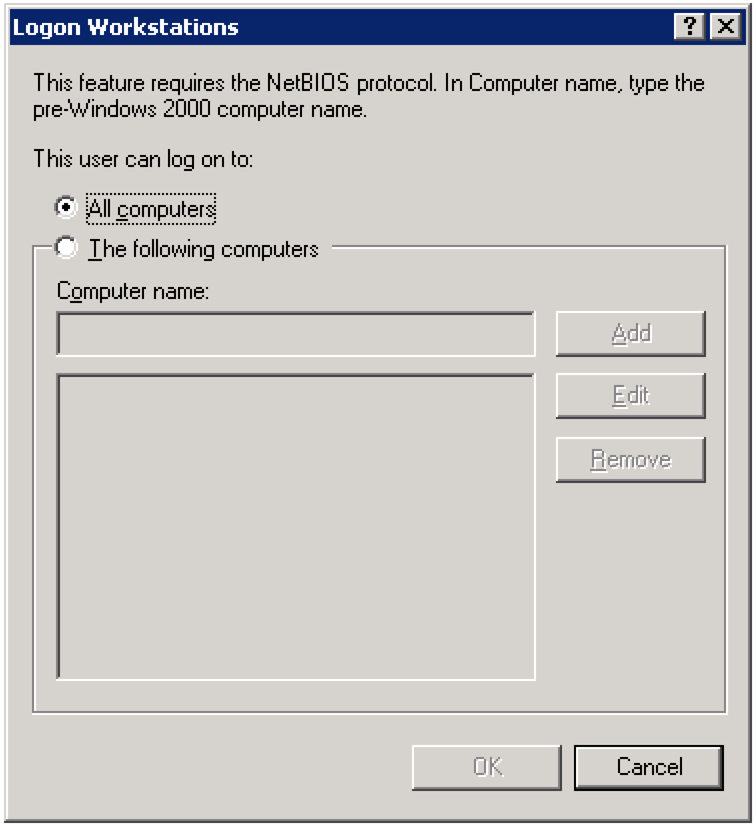
● Logon Permitted

○ Logon Denied

Sunday through Saturday from 12:00 AM to 12:00 AM

Account Tab -- Log On To

- **Log On To** restrictions on physical location



This feature requires the NetBIOS protocol. In Computer name, type the pre-Windows 2000 computer name.

This user can log on to:

● All computers

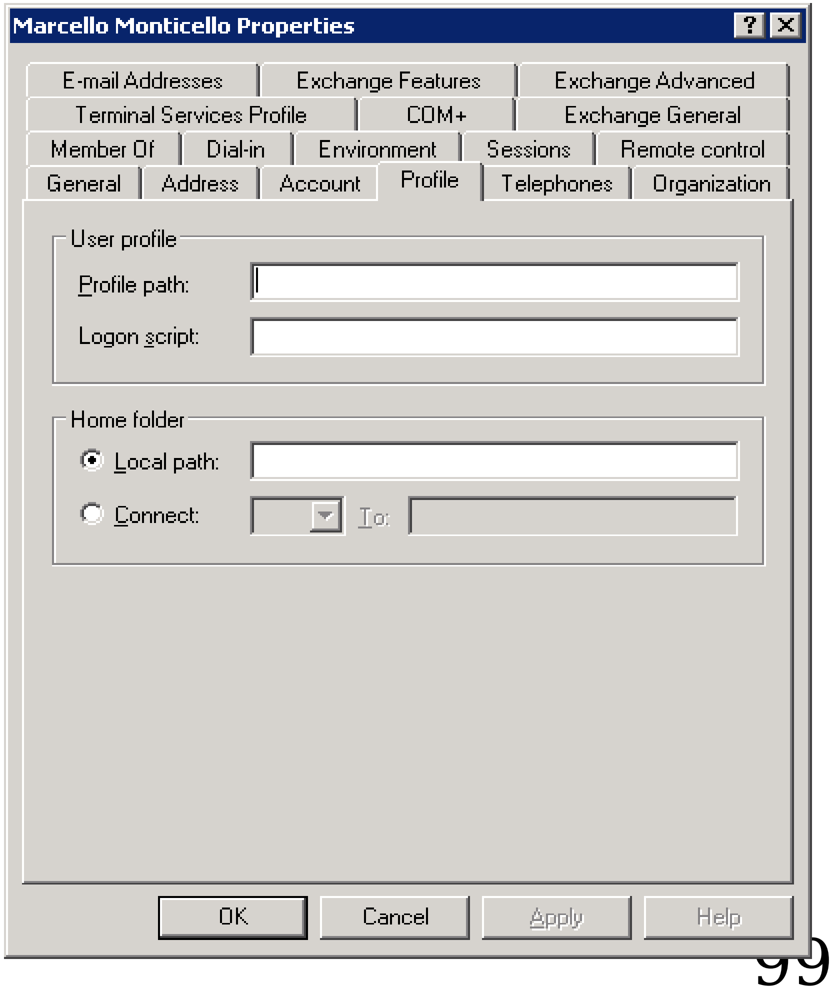
○ The following computers

Computer name:

Profile Tab

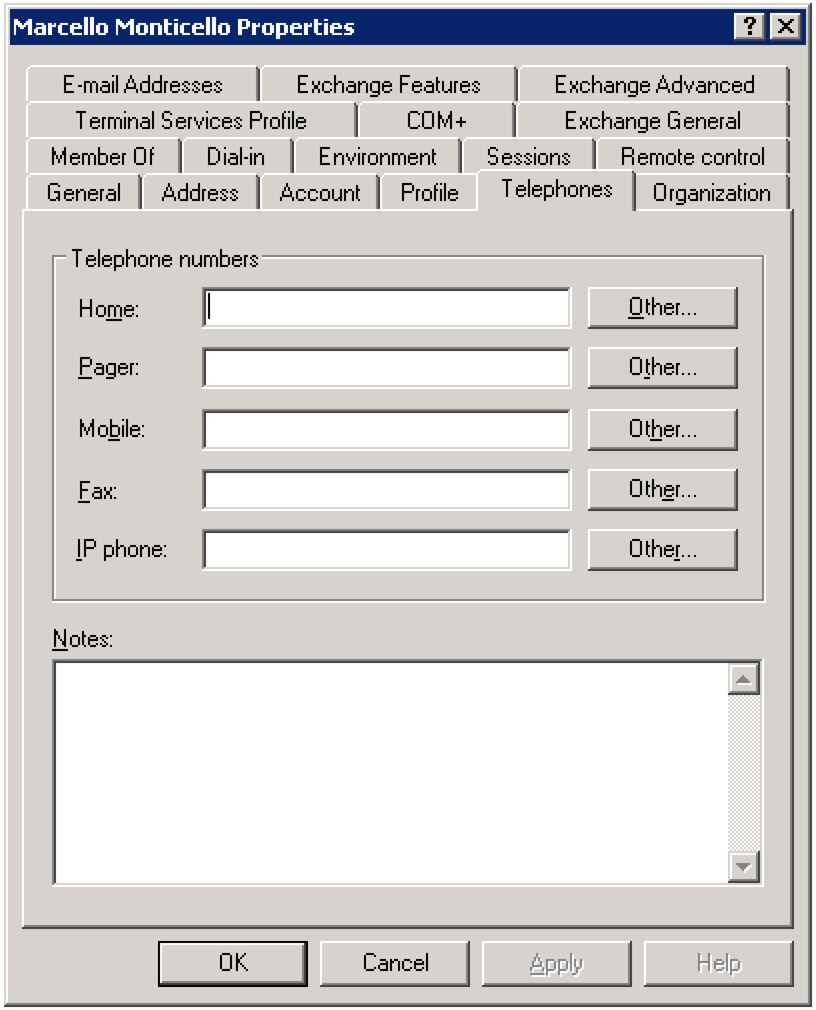
- Defines path to user profiles stored on share
  - Collection of settings and options that specify a user's desktop and all other user-definable settings for a user's work environment
  - Roaming user profiles or mandatory profiles **(.man)** (normally stored on network share)

- Logon scripts to execute at logon time
- Home folder where files saved



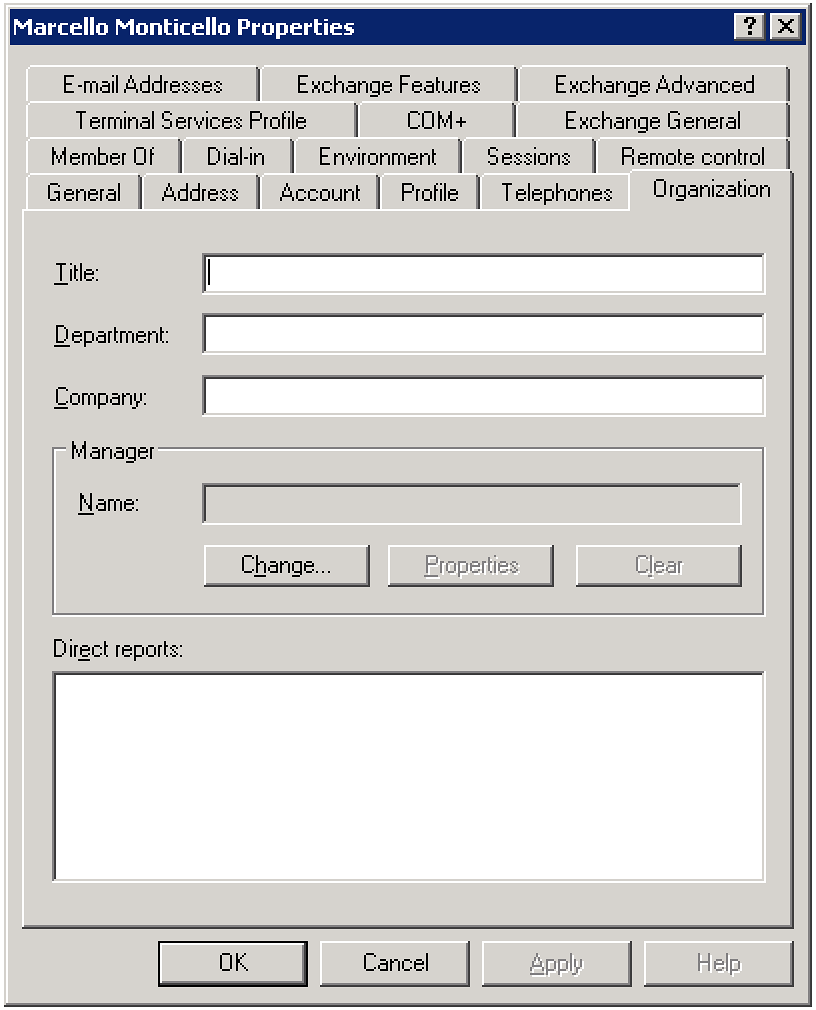
Telephone Tab

- Personal properties tab
- Documents home, pager, mobile, fax, and IP telephone numbers, and comments



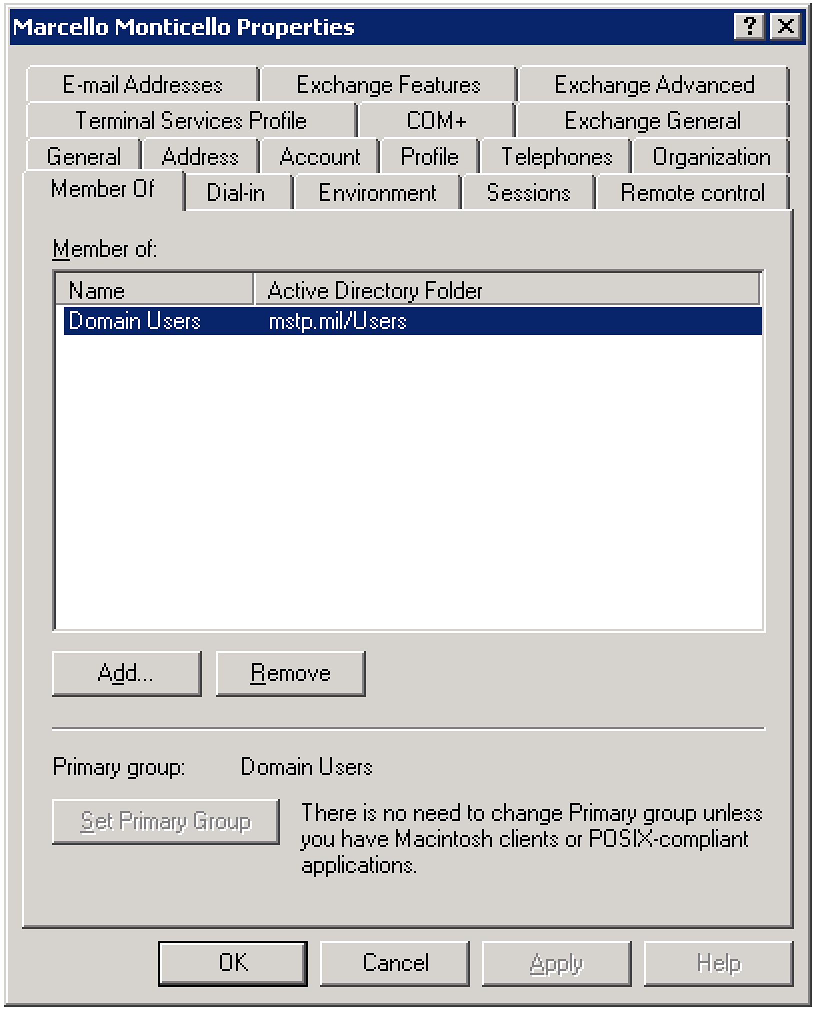
Organization Tab

- Personal properties tab
- Records title, department, company, manager, and direct reports


Marcello Monticello Properties

Members Of Tab

- Documents the groups the user belongs to



Marcello Monticello Properties

Member of:

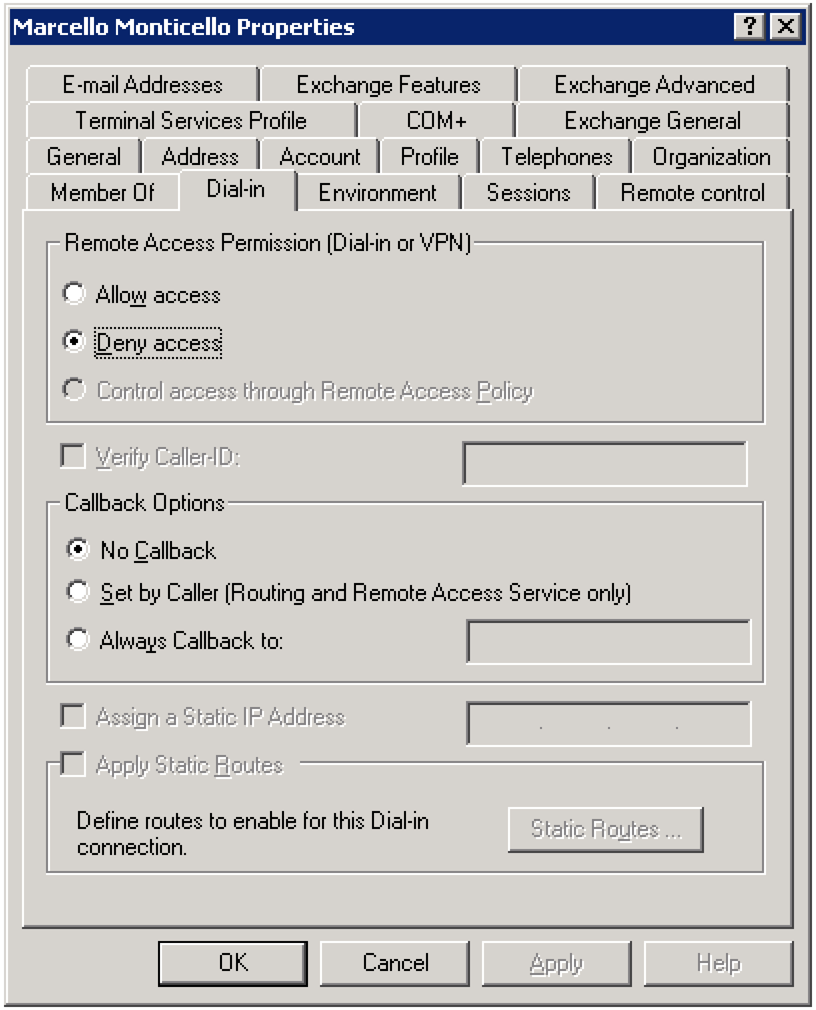
Name	Active Directory Folder
Domain Users	mstp.mil/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

Dial-In Tab

- Controls user dial-in connection ability
- Allow or deny access
- Verify Caller-ID w/proper equipment
- Callback security options -- No Call Back, Set By Caller (RRAS only), or Always Callback To



Marcello Monticello Properties

Remote Access Permission (Dial-in or VPN)

○ Allow access

● Deny access

○ Control access through Remote Access Policy

□ Verify Caller-ID:

Callback Options

● No Callback

○ Set by Caller (Routing and Remote Access Service only)

○ Always Callback to:

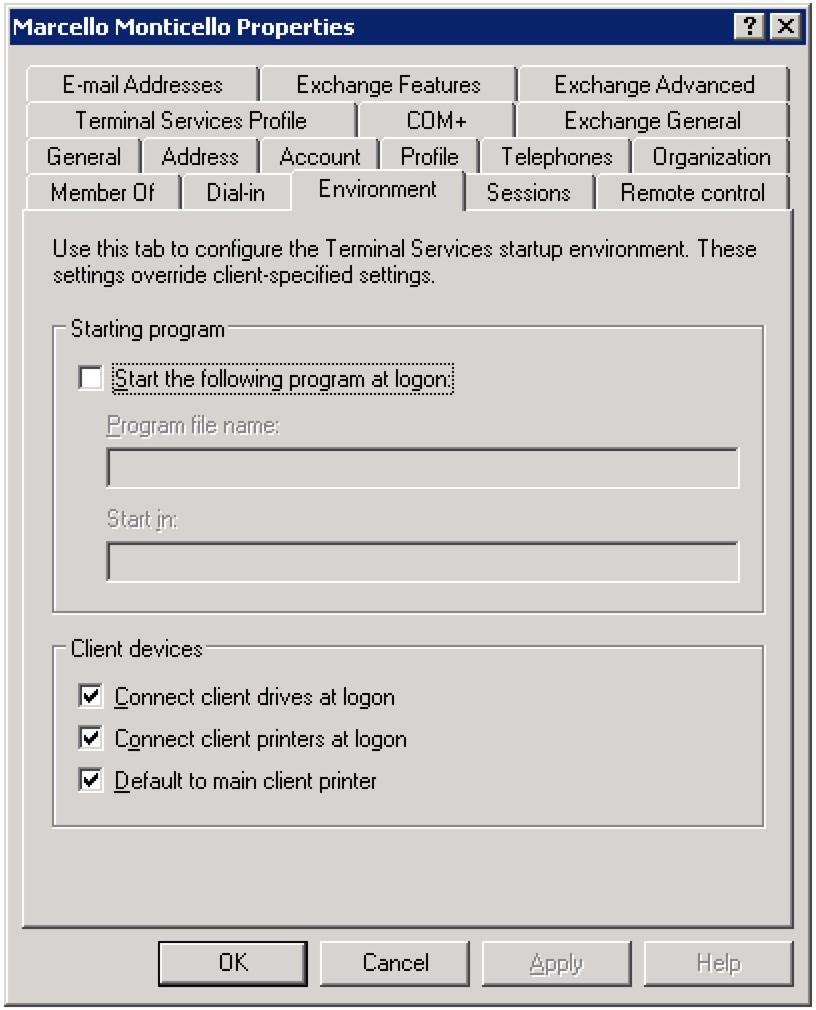
□ Assign a Static IP Address

□ Apply Static Routes

Define routes to enable for this Dial-in connection.

Environment Tab

- Settings for creating client working environment to start applications & locate local client drives



Marcello Monticello Properties

Use this tab to configure the Terminal Services startup environment. These settings override client-specified settings.

Starting program

□ Start the following program at logon:

Program file name:

Start in:

Client devices

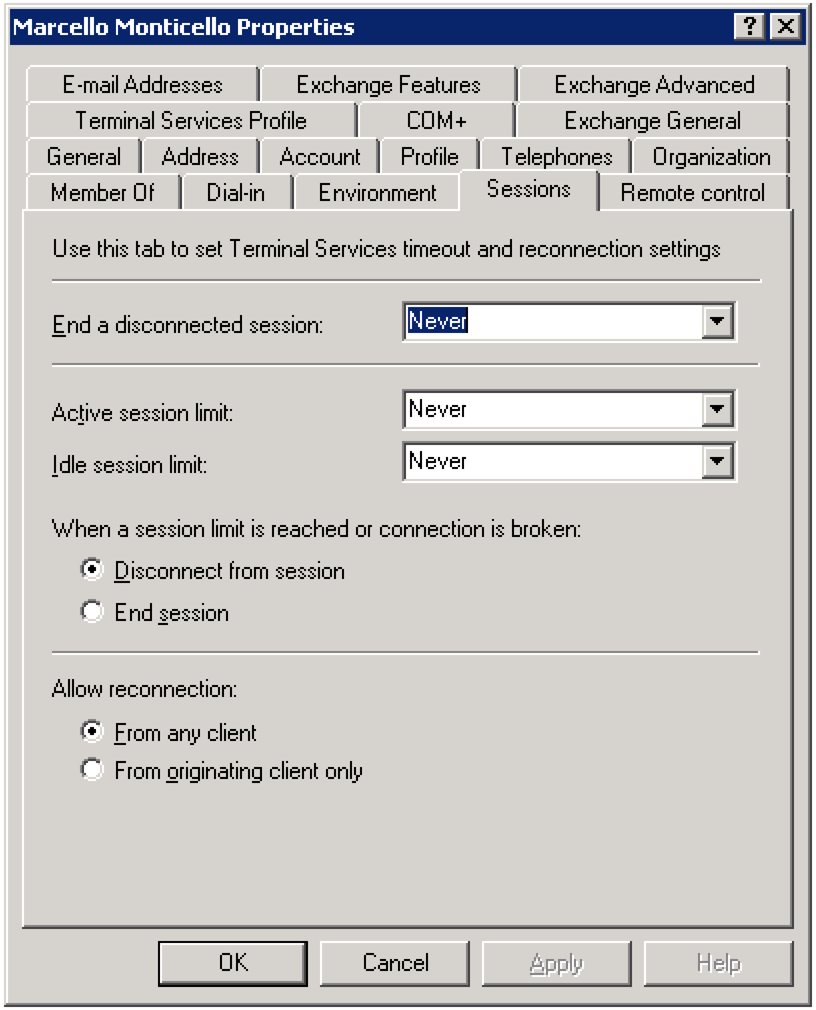
☑ Connect client drives at logon

☑ Connect client printers at logon

☑ Default to main client printer

Sessions Tab

- Settings for limiting length of sessions based on current state (active, idle, or disconnected)



Marcello Monticello Properties

Use this tab to set Terminal Services timeout and reconnection settings

End a disconnected session: Never

Active session limit: Never

Idle session limit: Never

When a session limit is reached or connection is broken:

● Disconnect from session

○ End session

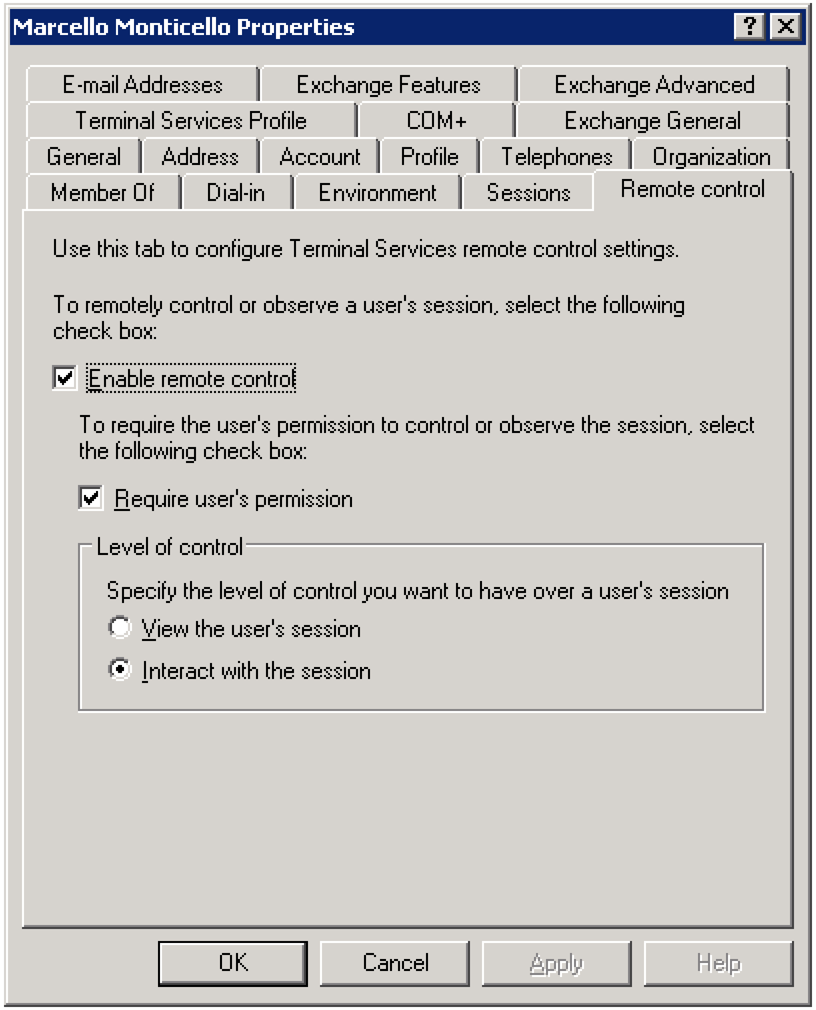
Allow reconnection:

● From any client

○ From originating client only

Remote Control Tab

- Monitor actions of client logged on Terminal Server using remote control from another session; Actively control client session
- Provides functionality similar to SMS remote control



Marcello Monticello Properties

Use this tab to configure Terminal Services remote control settings.

To remotely control or observe a user's session, select the following check box:

☑ Enable remote control

To require the user's permission to control or observe the session, select the following check box:

☑ Require user's permission

Level of control

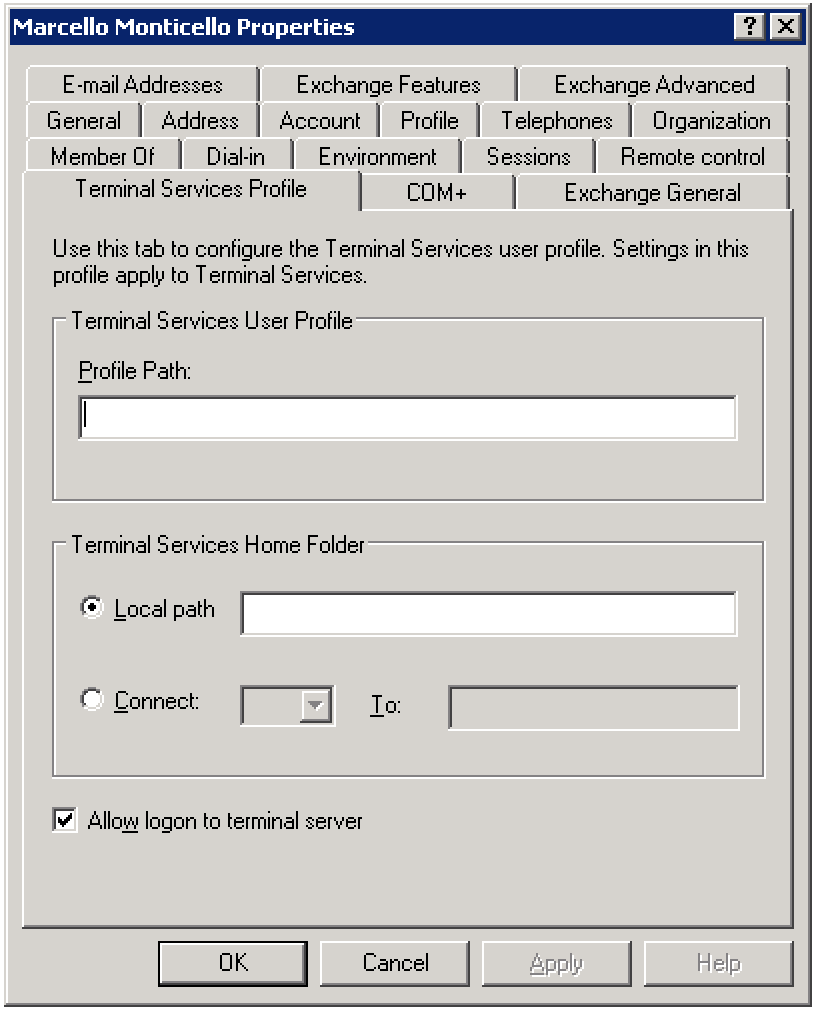
Specify the level of control you want to have over a user's session

○ View the user's session

● Interact with the session

Terminal Services Profile Tab

- Assigns a profile to a user to apply to Terminal sessions



Use this tab to configure the Terminal Services user profile. Settings in this profile apply to Terminal Services.

Terminal Services User Profile

Profile Path:

Terminal Services Home Folder

● Local path

○ Connect: To:

☑ Allow logon to terminal server

Administrative Tasks

- Highlight name; Use Action menu to select
- <u>Disable</u> don’t need account, but will use again
- <u>Rename</u> retain all rights, permissions, group memberships, & most properties to reassign
- <u>Delete</u> account is no longer used
- <u>Resetting passwords</u> entering new password
  - Do NOT need to know the old password
- <u>Unlocking</u> accounts violating policy

Group Types

- Use AD Users and Computers to create
- Groups – collections of user accounts to ease of administration when assigning permissions (Security) or functions unrelated to security (Distribution)
- Security groups have capabilities of a distribution group included

Group Scopes

- Domain local group (like NT)
- Global groups (like NT)
- Universal groups: Access resource any domain
  - Native mode only (only 2000 O/S in domain)
- Some local, global and universal groups created by default
  - Administrators, Users, Domain Admins, Domain Users, and Enterprise Admins
  - Can NOT rename default groups
  - Can NOT delete any built-in or system groups

Domain Local Groups

- Purpose -- to control access to resources by assigning permissions within one domain
- Created on 2003 computers part of a domain and stored in domain directory database (SAM) on DC on which created
- If create a local group in CSS domain, maintained in directory database for CSS
- Non-domain local groups created on Professional/Stand-alone servers & apply to that computer

Permissions and Membership

- Domain Local groups on 2003 servers DCs can be assigned permissions on any resource on any domain controller
- Permissions assigned to resources on stand-alone servers, member servers or workstation only apply to those machines
- Membership in domain local groups can include members from any domain in the tree/forest

Global Groups

- To organize users performing similar tasks or network access requirements
- Only be created on domain controllers
- Assign permissions to gain access to resources that are located in any domain
- Membership only includes users from the domain in which you created the global group
- Users from other domains can not be placed in another domain’s global group

Global Group Nesting

- Global group nesting is permitted meaning global groups can be put into other global groups to create a hierarchy of groups
- Unlimited levels of nesting ONLY in Native mode of 2000
- Nesting reduces network traffic between domains
- Nesting simplifies administration in a domain tree

Universal Groups

- Used to assign permissions/give access to related resources in multiple domains
- Available in Native mode only
- Membership is members from any domain
- Use when membership is static since changes will be replicated increasing network traffic
- Add global to universal groups, assign permissions for resources to universal

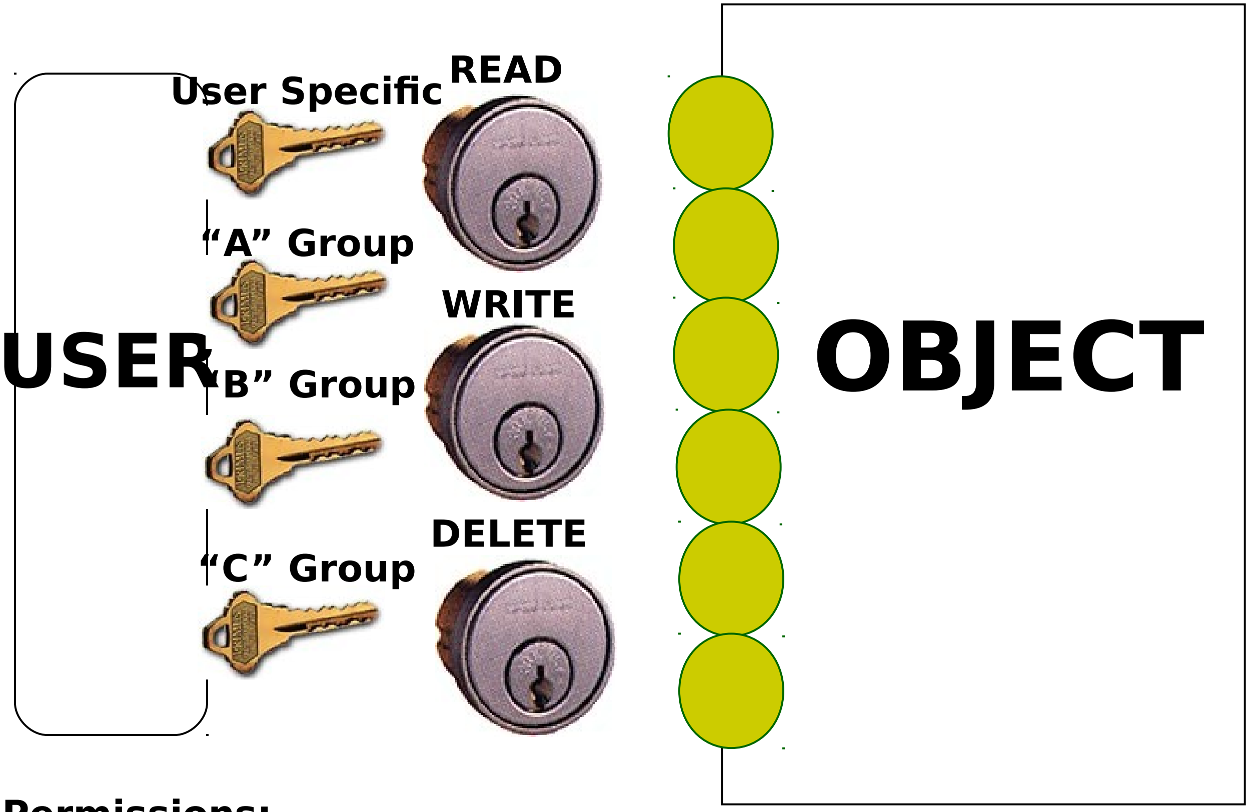
Rules to Dealing With Groups

- Prescribed method of applying permissions
- U-GG-DL(UG)-Permissions
  - Users go into global groups
  - Global groups are put into domain local groups or universal groups
  - Domain local groups or universal groups are given the permissions

Access Tokens and ACL's

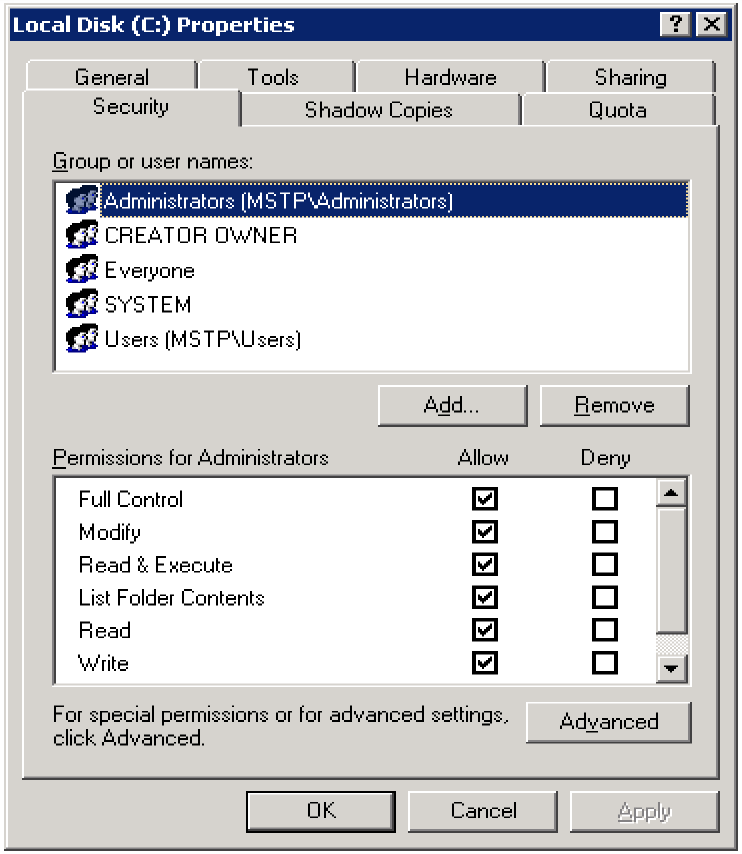
ACCESS TOKEN

ACCESS CONTROL LIST



Permissions:
Share – responsible for controlling remote access to local resources. A share is a network resource: it is an object in itself which points to the resource object.
NTFS – Affect both local and remote access to a given object.

Security



Local Disk (C:) Properties

General | Tools | Hardware | Sharing | Security | Shadow Copies | Quota

Group or user names:

- Administrators (MSTP\Administrators)
- CREATOR OWNER
- Everyone
- SYSTEM
- Users (MSTP\Users)

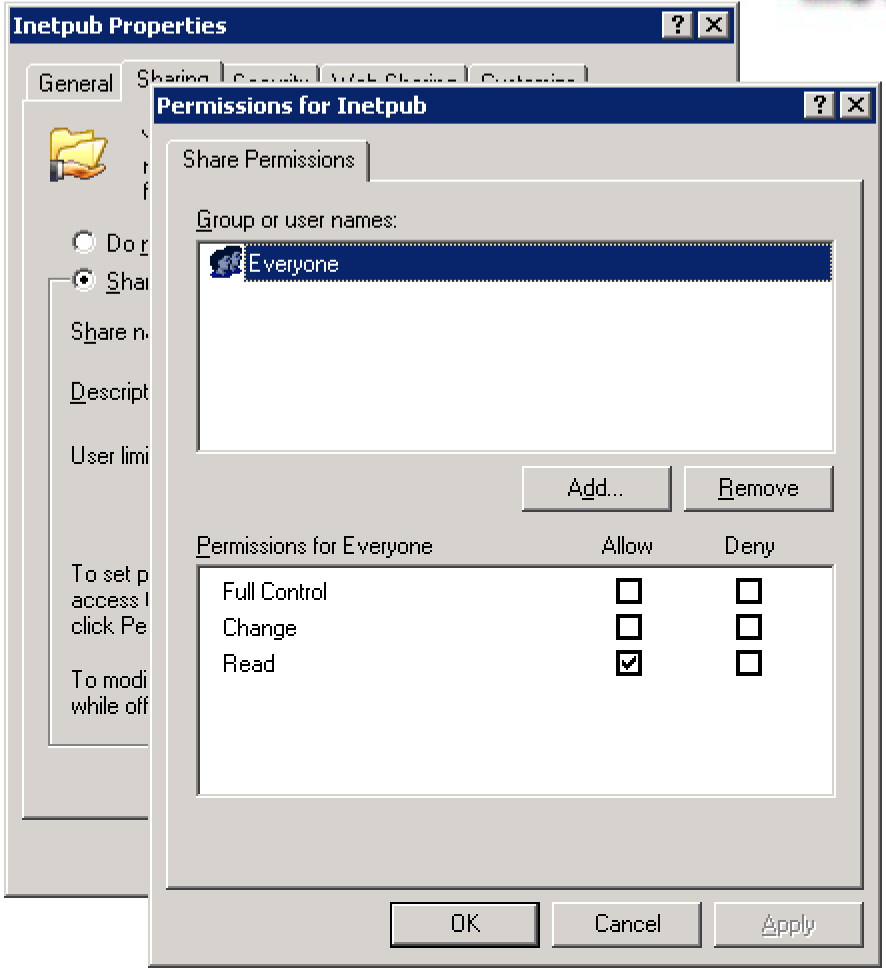
Add... | Remove

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

For special permissions or for advanced settings, click Advanced.

Advanced

OK | Cancel | Apply



Inetpub Properties

General | Sharing

○ Do r
● Shar

Share n

Descript

User limi

To set p access l click Pe

To modi while off

Permissions for Inetpub

Share Permissions

Group or user names:

- Everyone

Add... | Remove

Permissions for Everyone	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

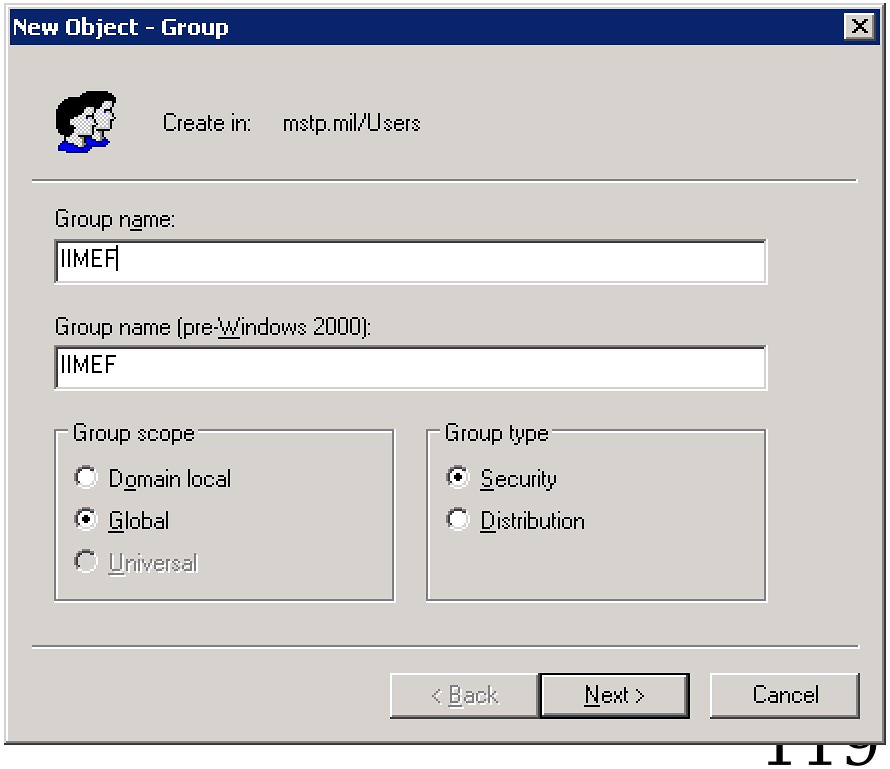
OK | Cancel | Apply

W2K performs the following authority check:

1. **Checks for No Access. If No Access is found, the user is denied access.**
2. **Checks for the specific granting of access based on user and any groups. If found, the user is granted access.**
3. **If neither No Access or service permission is found, the default of No Access is used, and thus, the user is denied access.**

Creating Groups

- Use AD Users and Computers
- Create in USERS container or OU
- Action Menu, New/Group
- In New Object – Group dialog box
  - Group name pertinent to asset/resource
    - **Note there is no different in icons to distinguish between local or global groups (only group/user)**
  - Group name for pre-2000
  - Group scope
  - Group type
- Users can't be added until group is created


New Object - Group

Create in: mstp.mil/Users

Group name:
IIMEF

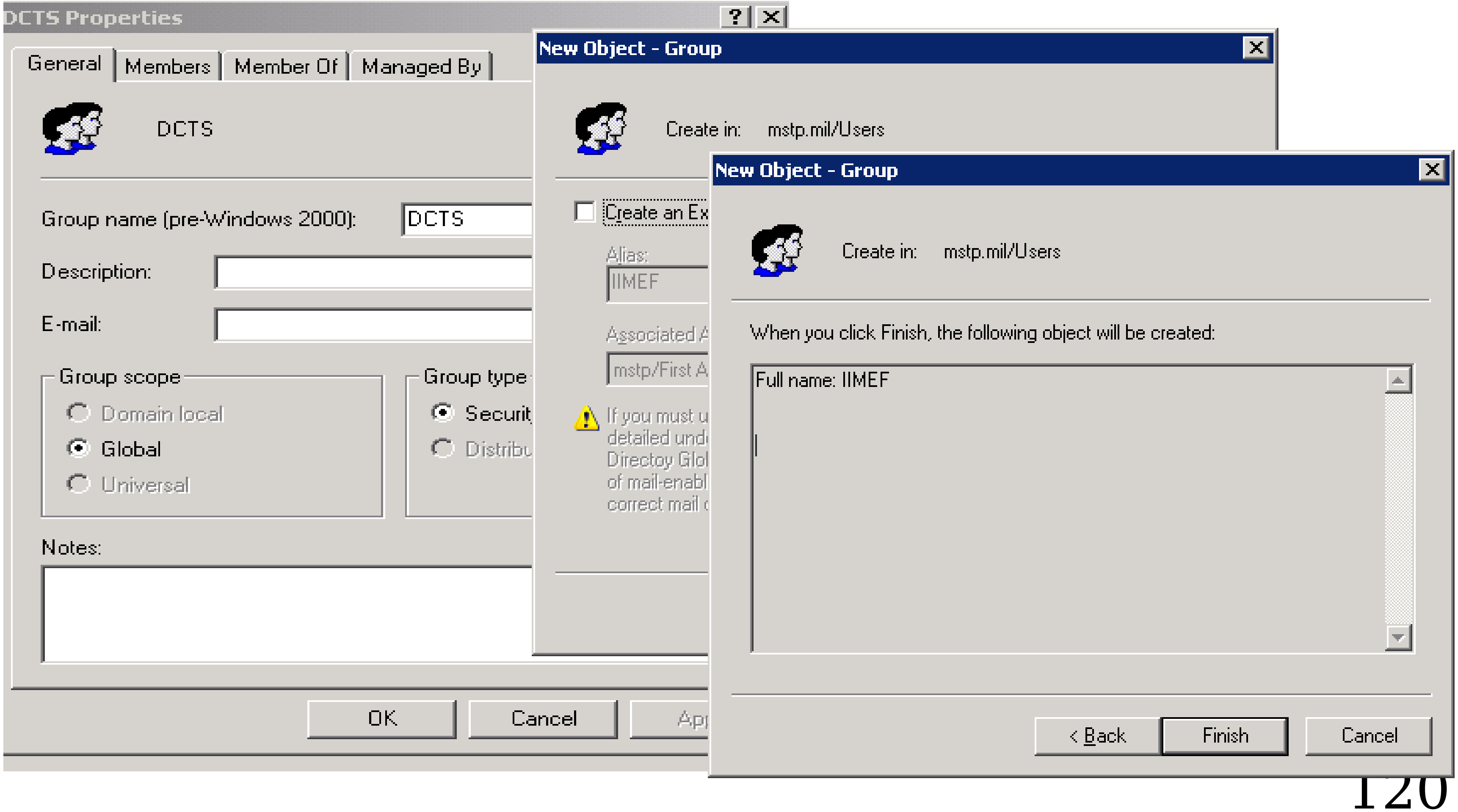
Group name (pre-Windows 2000):
IIMEF

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Group Properties

- Double-click group for group properties
- Can add Description, email and additional notes



DCTS

Group name (pre-Windows 2000): DCTS

Description:

E-mail:

Group scope
○ Domain local
● Global
○ Universal

Group type
● Securit
○ Distribu

Notes:

Create in: mstp.mil/Users

□ Create an Ex

Alias: IIMEF

Associated A

mstp/First A

If you must u
detailed und
Directoy Glol
of mail-enabl
correct mail c

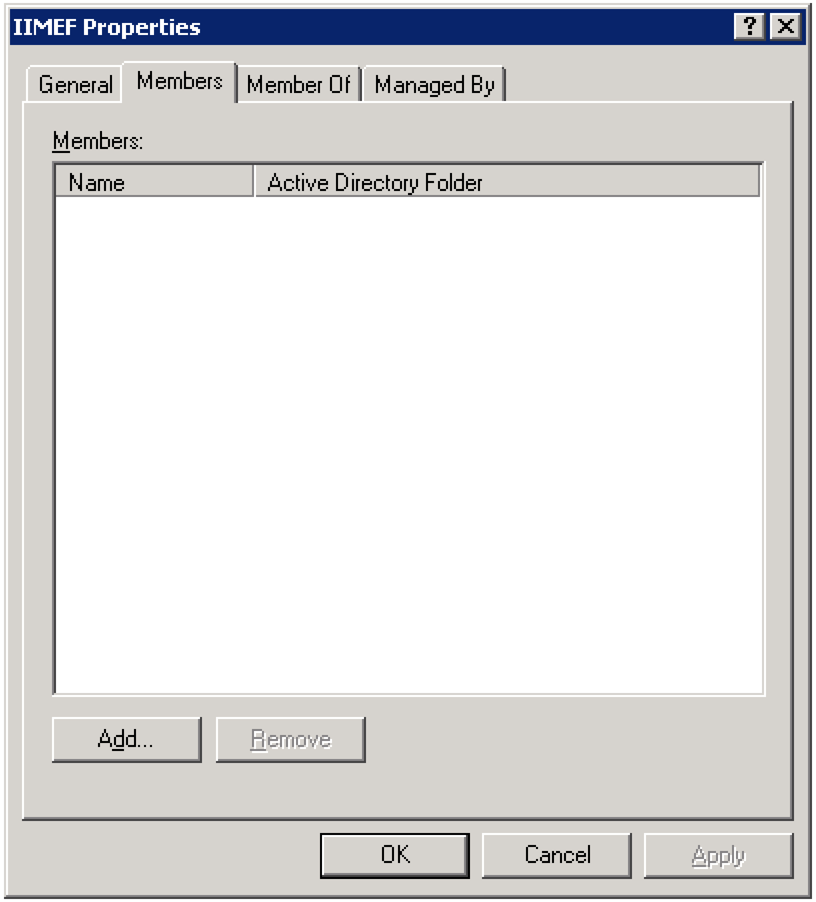
Create in: mstp.mil/Users

When you click Finish, the following object will be created:

Full name: IIMEF

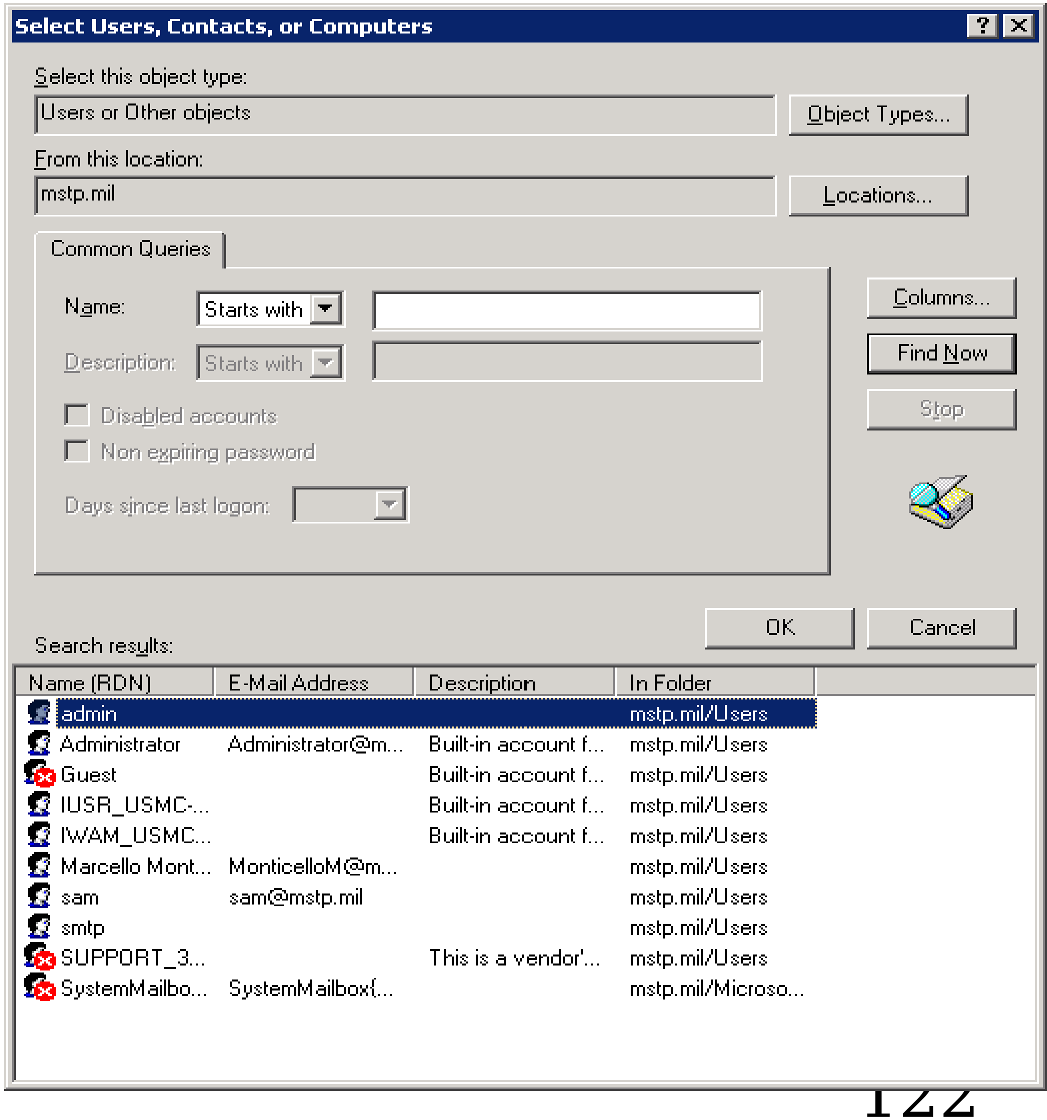
Add/Remove Members to Groups

- In Properties click Members tab; Click Add
- To remove, highlight user and use REMOVE button
- If creating non-domain local groups on Professional, group creation is similar to NT



Adding Members to Groups

- In Select Users, Contacts, or Computers dialog box, highlight the account you want to place in the group, and click add
- Once listed in bottom of dialog box, click OK



Select this object type: Users or Other objects

From this location: mstp.mil

Name: Starts with

Description: Starts with

☐ Disabled accounts

☐ Non expiring password

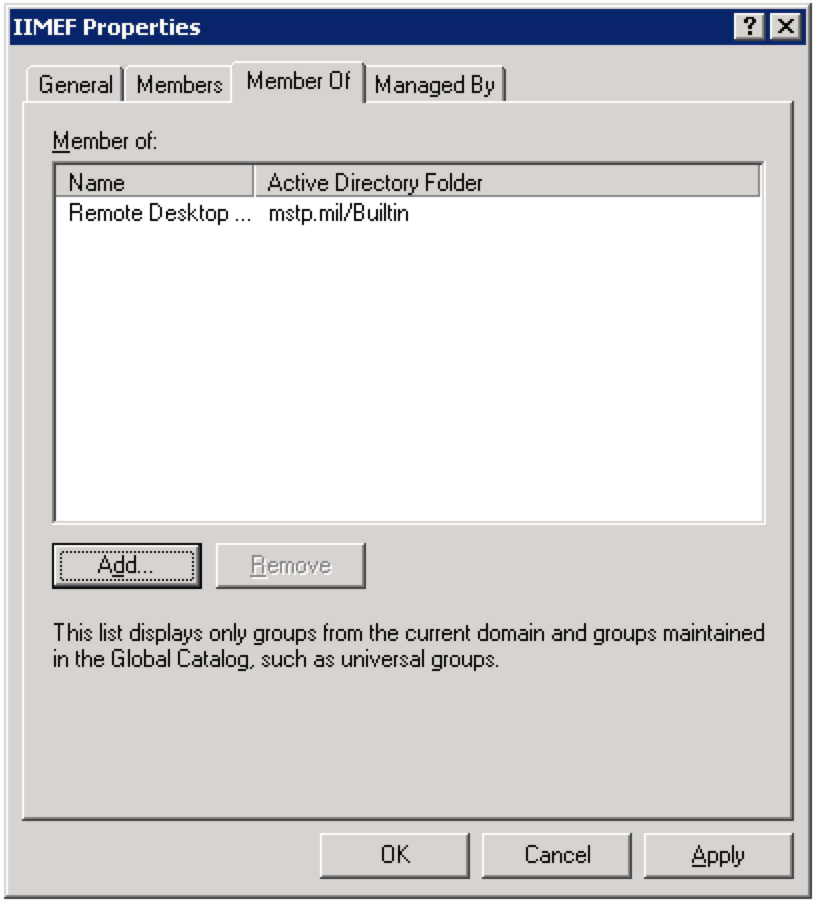
Days since last logon:

Search results:

Name (RDN)	E-Mail Address	Description	In Folder
admin			mstp.mil/Users
Administrator	Administrator@m...	Built-in account f...	mstp.mil/Users
Guest		Built-in account f...	mstp.mil/Users
IUSR_USMC-...		Built-in account f...	mstp.mil/Users
IWAM_USMC...		Built-in account f...	mstp.mil/Users
Marcello Mont...	MonticelloM@m...		mstp.mil/Users
sam	sam@mstp.mil		mstp.mil/Users
smtp			mstp.mil/Users
SUPPORT_3...		This is a vendor'...	mstp.mil/Users
SystemMailbo...	SystemMailbox{...		mstp.mil/Microso...

Member Of Tab

- If the group is a member of another group
- Global Group or Domain Local Group



IIMEF Properties

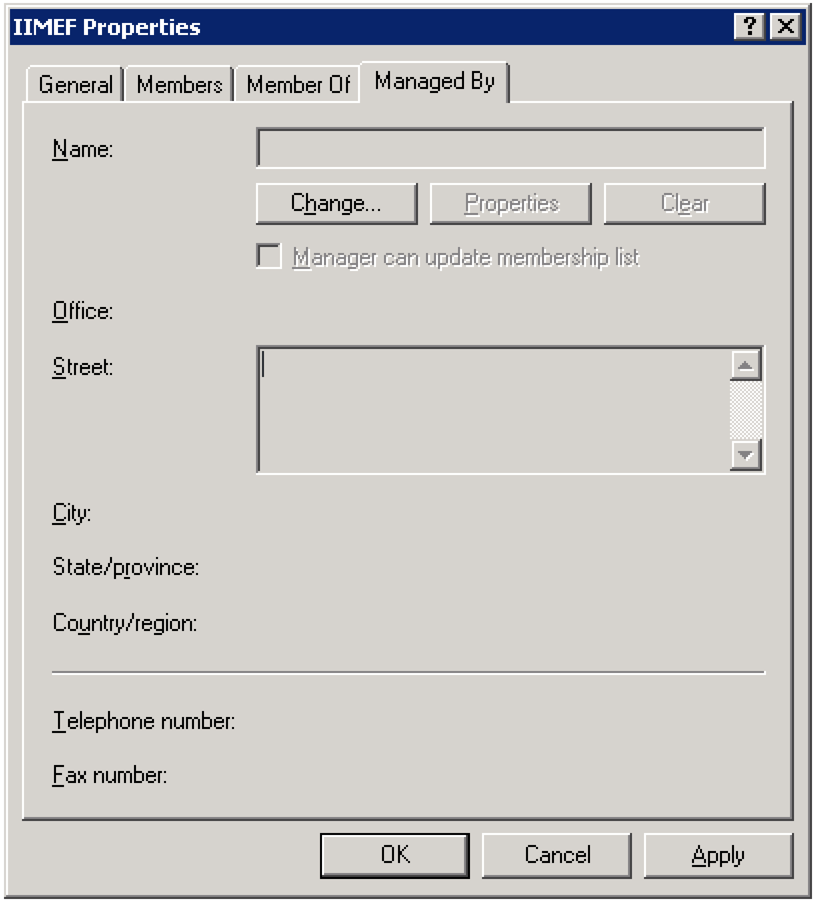
Member of:

Name	Active Directory Folder
Remote Desktop ...	mstp.mil/Builtin

This list displays only groups from the current domain and groups maintained in the Global Catalog, such as universal groups.

Managed By Tab

- To set if someone other than an administrator will take care of the group definition



REVIEW

Windows Server 2003 has a very flexible security architecture. In this session, you learned how Windows Server 2003 can play different roles on a network:

- Standalone server
- Domain controller
- Member server

You also learned that standalone servers and member servers can have their own user and group accounts and that those servers come with several accounts built right in. You learned how to create your own users and groups, and you learned how to control user accounts by defining a server’s local account policies. Finally, you learned how to use security auditing to keep tabs on how your servers are being used and by whom.

QUIZ YOURSELF

- **1.** What are the names of the built-in Windows Server 2003 user groups?
- **2.** What are the names of the built-in Windows Server 2003 users?
- **3.** How can you control the minimum length of passwords used by local users?
- **4.** How do you enable security auditing in Windows Server 2003?

GPO's

Group Policy (GP)

- Configuration settings that apply to one or more objects in AD
- Controls work environments for users
- Provisions
  - Auto delivery of applications to user for install
  - Delivers file/shortcuts to network/computer
  - Auto execution of tasks at designated times
  - Security settings for Account Policy, User Rights, Audit Policies, Event log, etc
  - Redirects folders to network locations

Group Policy Object Administration

- The Group Policy snap-in is GPO-specific
- This allows user to add a snap-in for each GPO that you want to administer for a site, domain or OU where the GPO is located
- 2003 registry settings cleaned and rewritten each time policy changes in difference to NT which had to be explicitly reversed
- Reapplied every 90 minutes by default

Group Policy Application

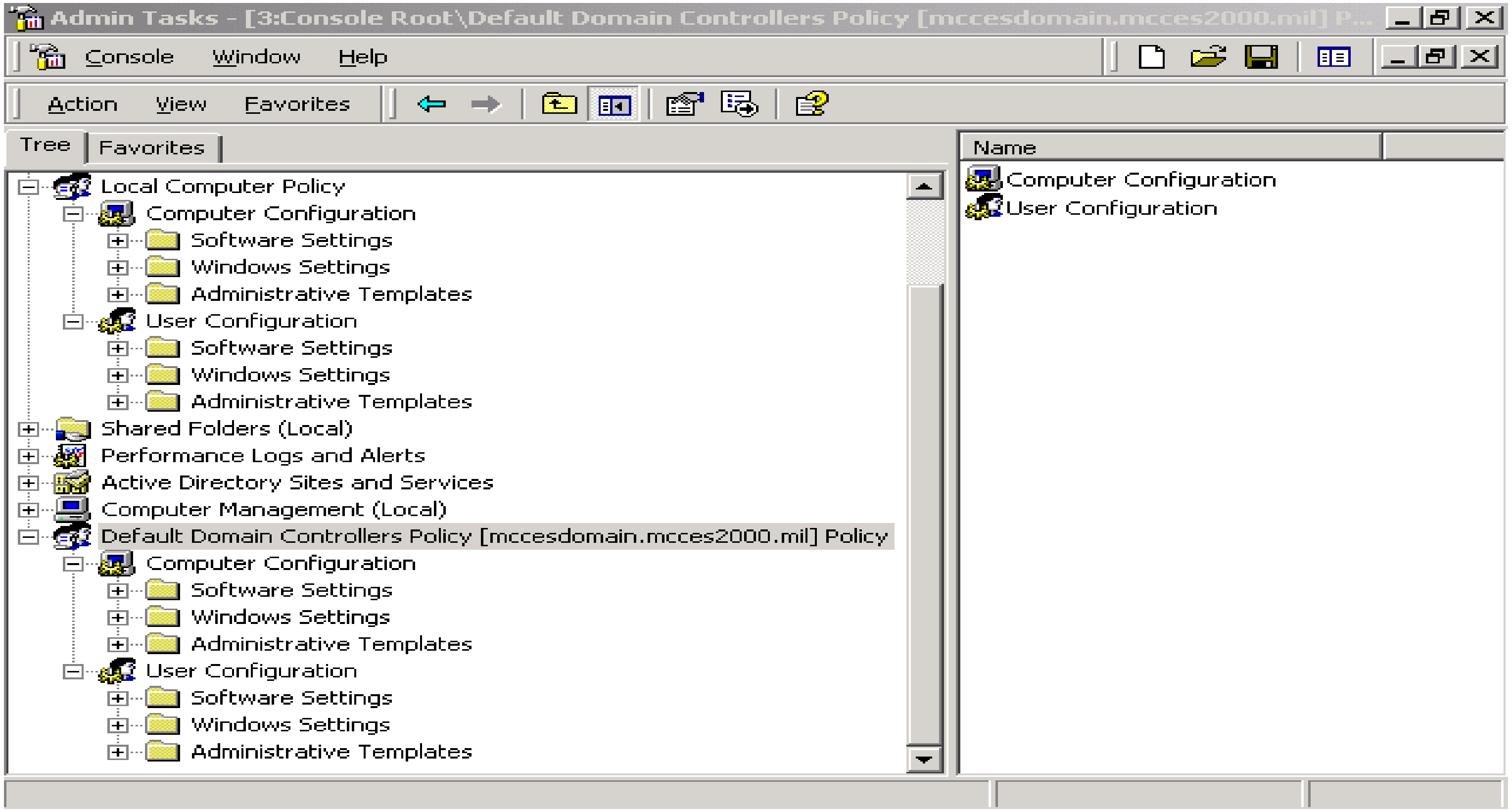
- Not part of domain -- local computer policy only
- Part of domain applied in a specific order
  - Windows NT policies from NETLOGON share
  - Local computer policy
  - SITE level policies
  - DOMAIN level policies
  - OU level policies
  - Child OU policies
- Exception -- account policies only at DOMAIN

Group Policy Association

- Multiple containers in AD can be associated with same GPO
- Single AD container can have more than one GPO
- The scope of the GPO depends on the membership in security groups

Group Policy Object

- Once create GPO, use Group Policy snap-in to edit settings for computers/users
- Two sections – Computer and User Config



Admin Tasks - [3:Console Root\Default Domain Controllers Policy [mccesdomain.mcces2000.mil] P...
Console
Window
Help
Action
View
Favorites
Tree
Favorites
Name

- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
- Shared Folders (Local)
- Performance Logs and Alerts
- Active Directory Sites and Services
- Computer Management (Local)
- Default Domain Controllers Policy [mccesdomain.mcces2000.mil] Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Computer Configuration
User Configuration

Group Policy Sections

- Computer Configuration (CC)
  - Customize user’s environment & enforce lockdown policies for computers
  - Policies applied when the O/S initializes
  - Apply to every user logging on a computer regardless of the OU the user belongs
- Sub sections include Software Settings, Windows Settings, and Administrative Templates

Group Policy Sections

- User Configuration (UC)
  - Customize the user’s environment
  - Enforce lockdown policies for users
  - Include desktop appearance, application settings, logon and logoff scripts, and assigned and published applications
  - Apply when the user logs on to the computer
- Sub sections include Software Settings, Windows Settings, and Administrative Templates

Software Settings

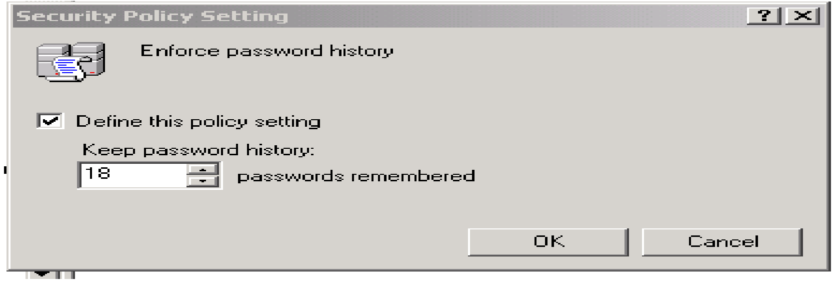
- Affects applications to which users can gain access
- Installations automatic by
  - Application assignment (upon connection the application will install automatically)
    - Computer Configuration Section
  - Application published (user has to use Add/Remove Programs to load the application) or assigned (application automatically installed)
    - User Configuration Section

Windows Settings -- Scripts

- Allows scripts and batch files to be run at specified times
  - startup or shutdown (Computer Configuration Section)
  - log on/off (User Configuration Section)
- Automating of repetitive tasks
- Order of Execution
  - Startup, log on, log off, shutdown

CC Windows Settings -- Security

- Sets security settings for the computer in many areas (each to be covered)
- Account Policies: set password & lockout policy
  - Enforce Password History/Password Uniqueness



Security Policy Setting

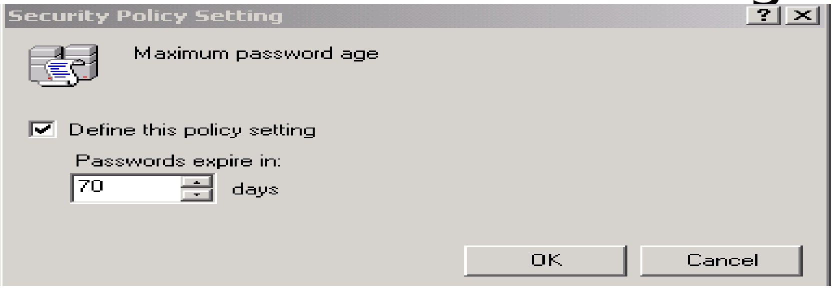
Enforce password history

☑ Define this policy setting

Keep password history:

18 passwords remembered

  - Maximum Password Age



Security Policy Setting

Maximum password age

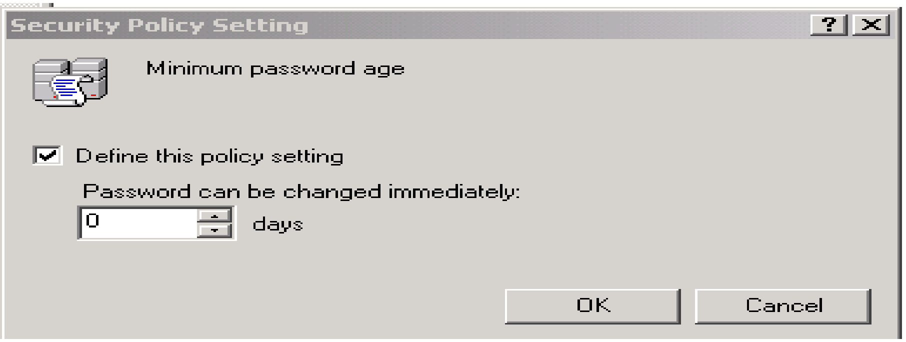
☑ Define this policy setting

Passwords expire in:

70 days

CC Security Settings -- Account

- Account Policies: set password & lockout policy
  - Minimum Password Age
  - Min



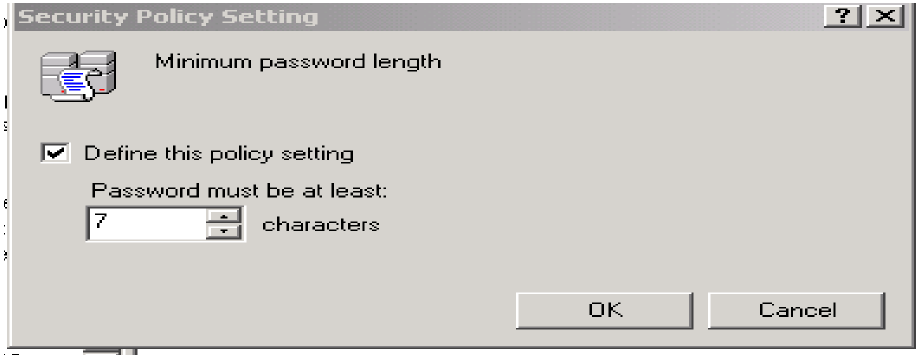
Security Policy Setting

Minimum password age

☑ Define this policy setting

Password can be changed immediately:

0 days



Security Policy Setting

Minimum password length

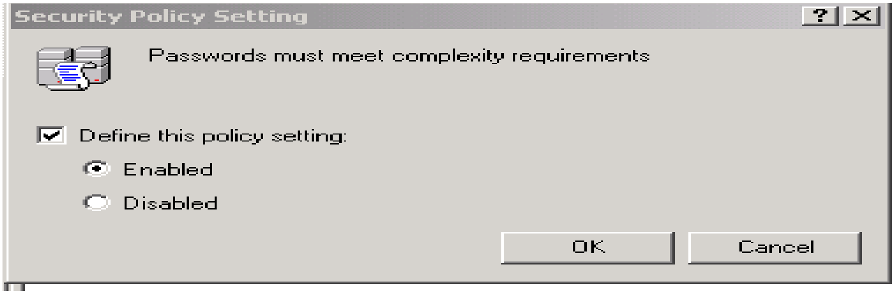
☑ Define this policy setting

Password must be at least:

7 characters

CC Security Settings -- Account

- Account Policies: set password & lockout policy
  - Complexity requirements such as 6 characters long, upper/lower case mixed
  - Reversible Encryption of user's password (user/all accts in a domain)
    - Normally Apple computers

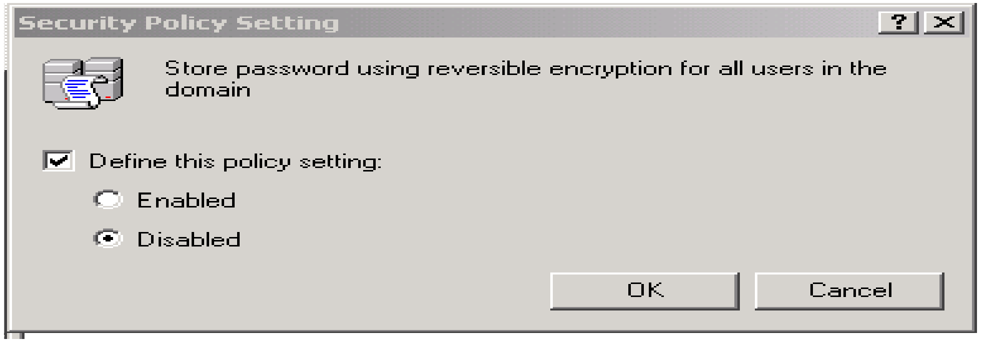


Passwords must meet complexity requirements

☑ Define this policy setting:

● Enabled

○ Disabled



Store password using reversible encryption for all users in the domain

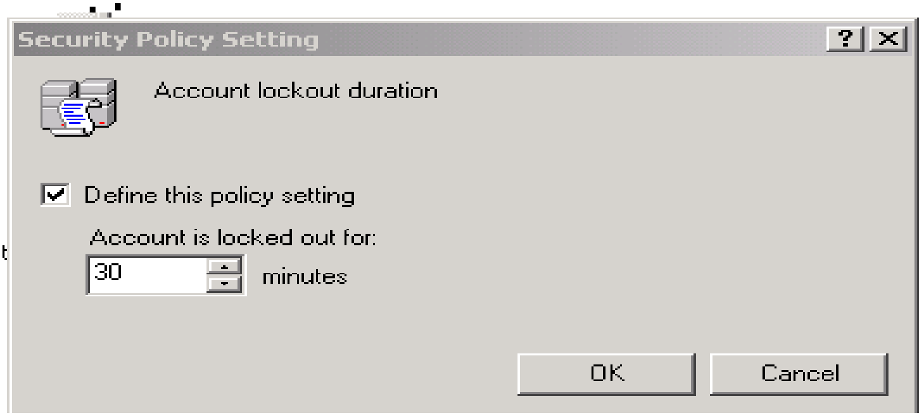
☑ Define this policy setting:

○ Enabled

● Disabled

CC Security Settings -- Lockout

- Account Lockout after successive unsuccessful logon attempts -- Du



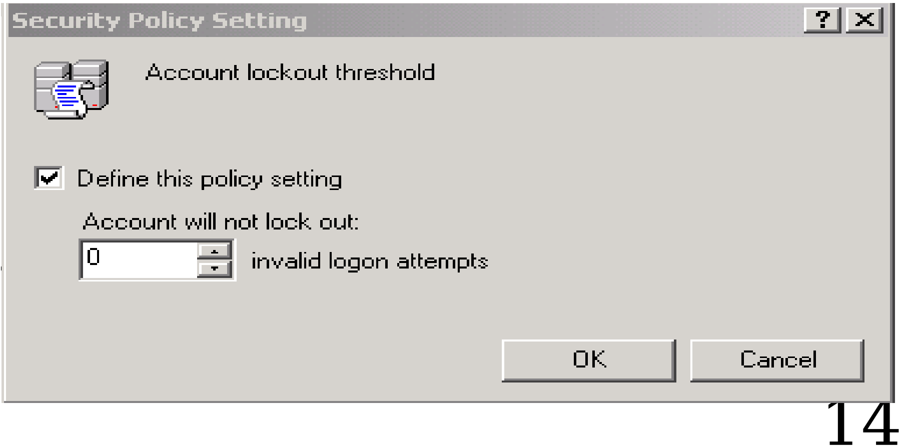
Account lockout duration

☑ Define this policy setting

Account is locked out for:

30 minutes

- Threshold



Account lockout threshold

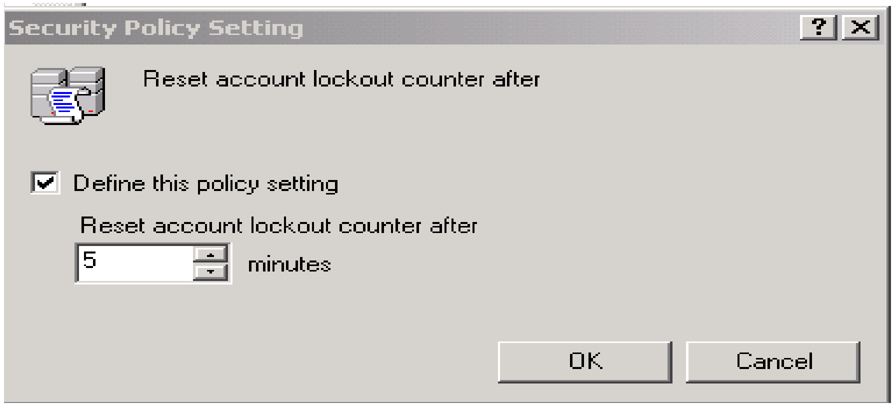
☑ Define this policy setting

Account will not lock out:

0 invalid logon attempts

CC Security Settings -- Lockout

- Account Lockout after successive unsuccessful logon attempts -- Reset



Security Policy Setting

Reset account lockout counter after

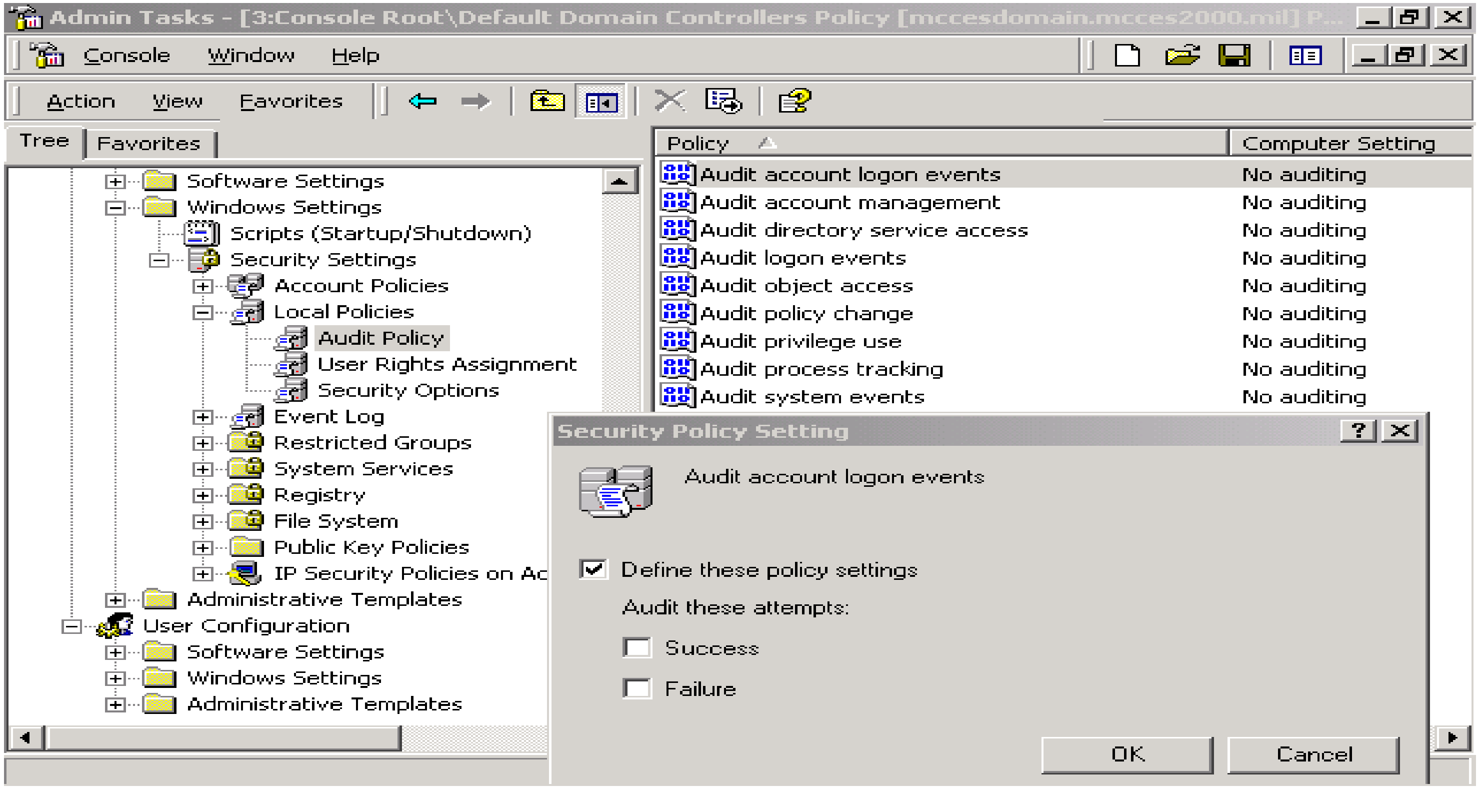
☑ Define this policy setting

Reset account lockout counter after

5 minutes

CC Security Settings -- Local Policies

- Auditing for the administrator to determine whether unauthorized users have accessed or attempted to access sensitive information



Policy	Computer Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Audit account logon events

☑ Define these policy settings

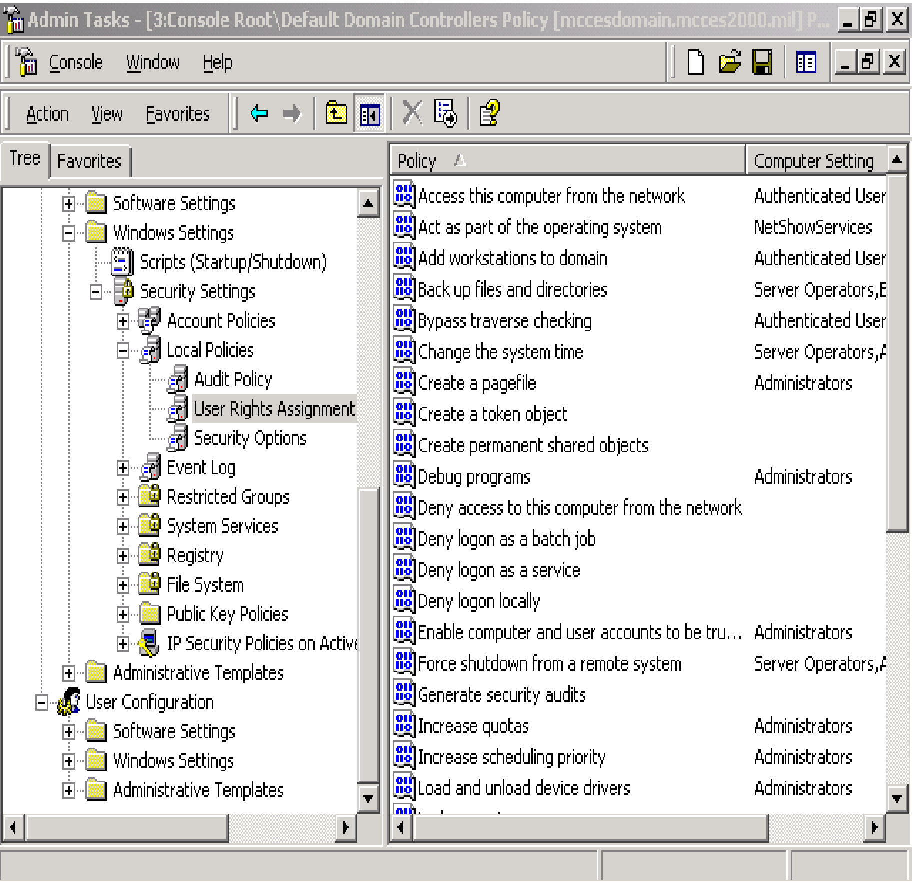
Audit these attempts:

□ Success

□ Failure

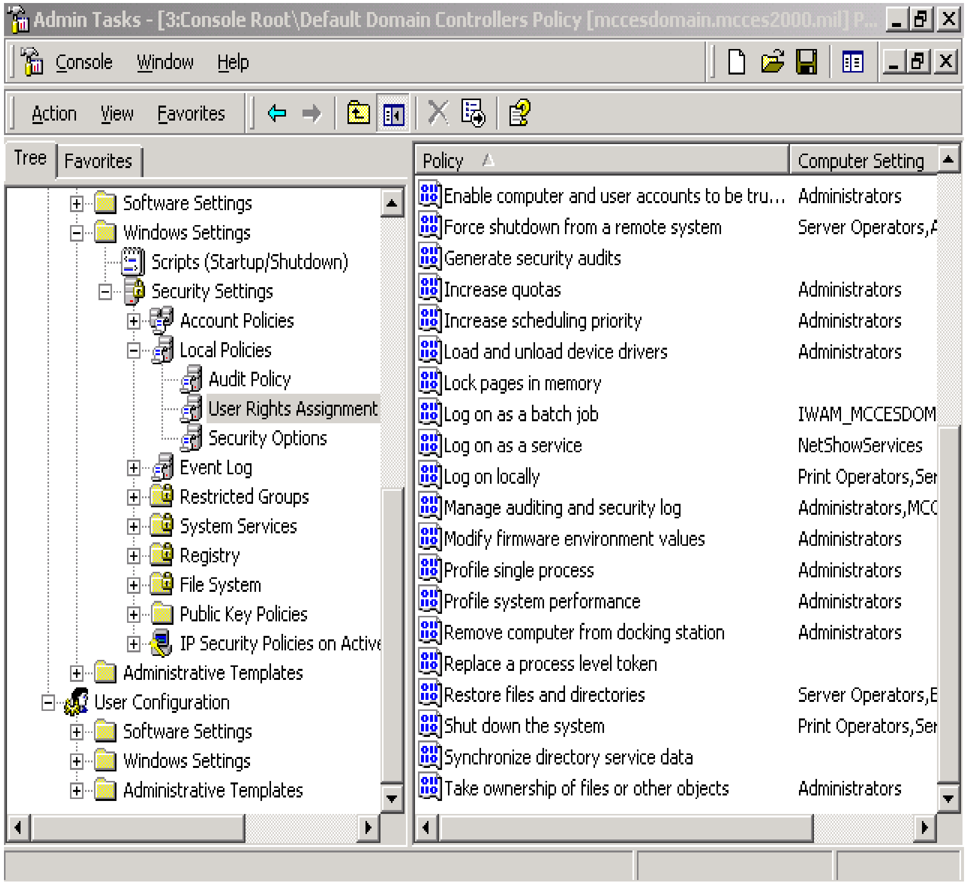
CC Security Settings -- Local Policies

- Set user rights authorizing users/groups to perform specific tasks on a 2000 computer


Admin Tasks - [3:Console Root\Default Domain Controllers Policy [mccesdomain.mcces2000.mil] P...
Console
Window
Help
Action
View
Favorites
Tree
Favorites

- Software Settings
- Windows Settings
  - Scripts (Startup/Shutdown)
  - Security Settings
    - Account Policies
    - Local Policies
      - Audit Policy
      - User Rights Assignment
      - Security Options
    - Event Log
    - Restricted Groups
    - System Services
    - Registry
    - File System
    - Public Key Policies
    - IP Security Policies on Active
- Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

Policy	Computer Setting
Access this computer from the network	Authenticated User
Act as part of the operating system	NetShowServices
Add workstations to domain	Authenticated User
Back up files and directories	Server Operators,E
Bypass traverse checking	Authenticated User
Change the system time	Server Operators,A
Create a pagefile	Administrators
Create a token object	
Create permanent shared objects	
Debug programs	Administrators
Deny access to this computer from the network	
Deny logon as a batch job	
Deny logon as a service	
Deny logon locally	
Enable computer and user accounts to be tru...	Administrators
Force shutdown from a remote system	Server Operators,A
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators

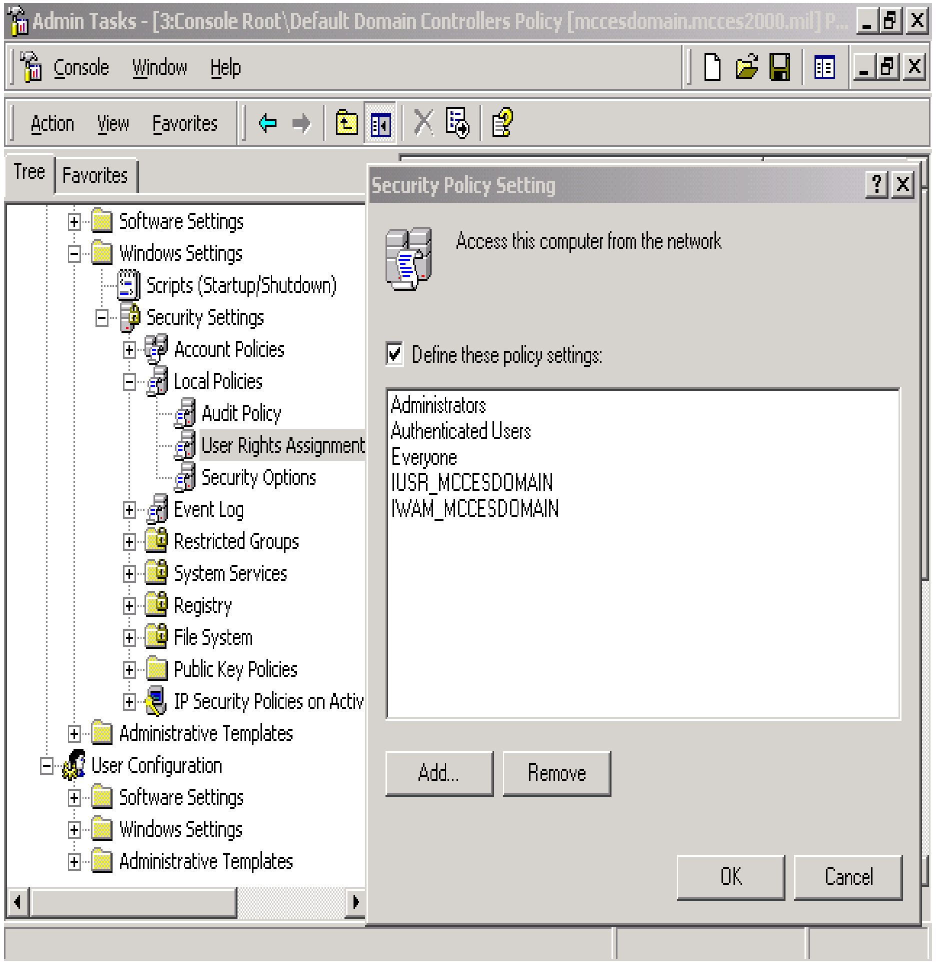

Admin Tasks - [3:Console Root\Default Domain Controllers Policy [mccesdomain.mcces2000.mil] P...
Console
Window
Help
Action
View
Favorites
Tree
Favorites

- Software Settings
- Windows Settings
  - Scripts (Startup/Shutdown)
  - Security Settings
    - Account Policies
    - Local Policies
      - Audit Policy
      - User Rights Assignment
      - Security Options
    - Event Log
    - Restricted Groups
    - System Services
    - Registry
    - File System
    - Public Key Policies
    - IP Security Policies on Active
- Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

Policy	Computer Setting
Enable computer and user accounts to be tru...	Administrators
Force shutdown from a remote system	Server Operators,A
Generate security audits	
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	
Log on as a batch job	IWAM_MCCESDOM
Log on as a service	NetShowServices
Log on locally	Print Operators,Ser
Manage auditing and security log	Administrators,MCC
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Administrators
Replace a process level token	
Restore files and directories	Server Operators,E
Shut down the system	Print Operators,Ser
Synchronize directory service data	
Take ownership of files or other objects	Administrators

CC Security Settings -- Local Policies

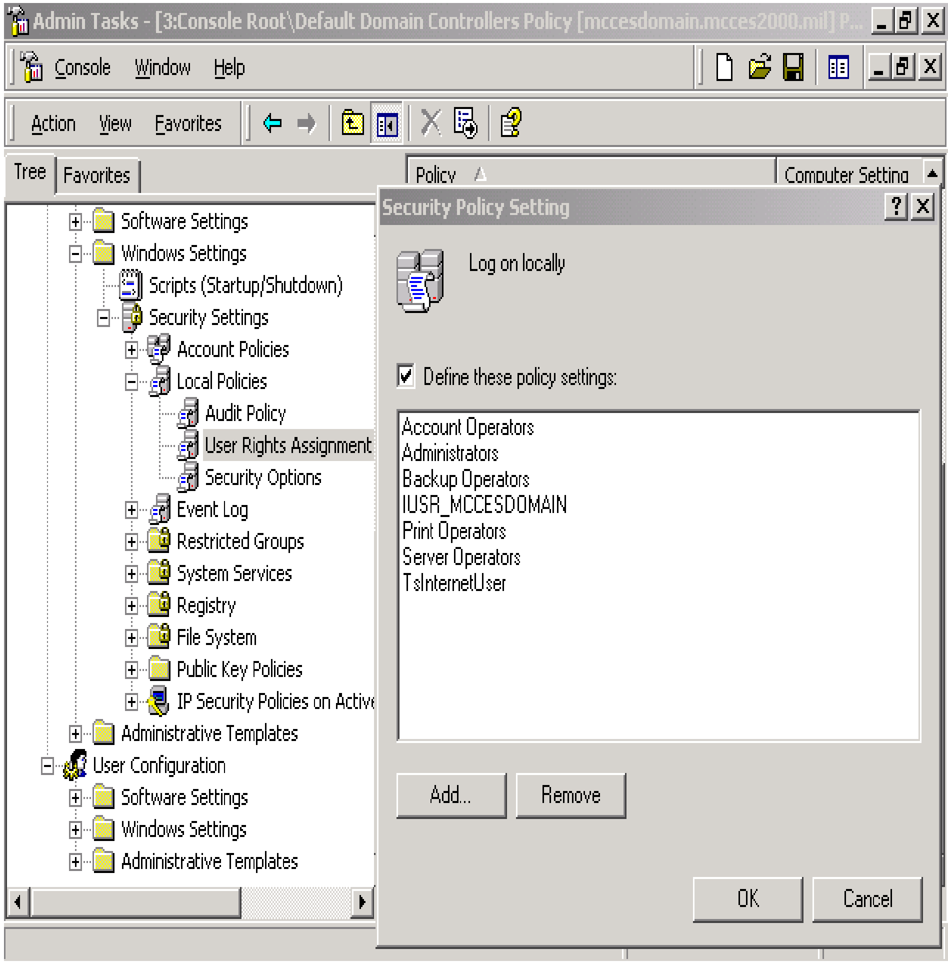
- Examples of Setting User Rights



Access this computer from the network

☑ Define these policy settings:

Administrators
Authenticated Users
Everyone
IUSR_MCCESDOMAIN
IWAM_MCCESDOMAIN



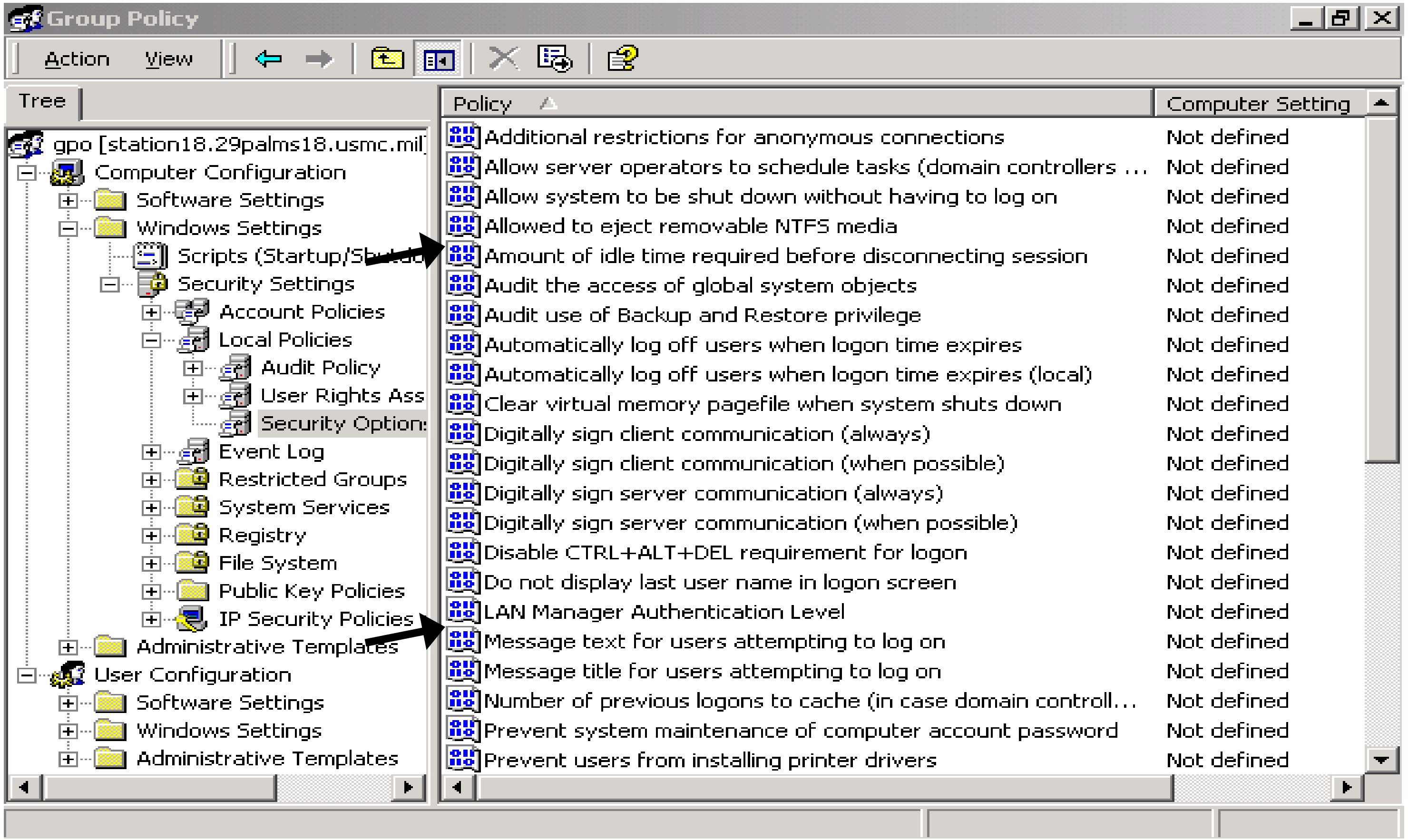
Log on locally

☑ Define these policy settings:

Account Operators
Administrators
Backup Operators
IUSR_MCCESDOMAIN
Print Operators
Server Operators
TsInternetUser

CC Security Options

- Varied options with security primarily covered in System Policy Editor

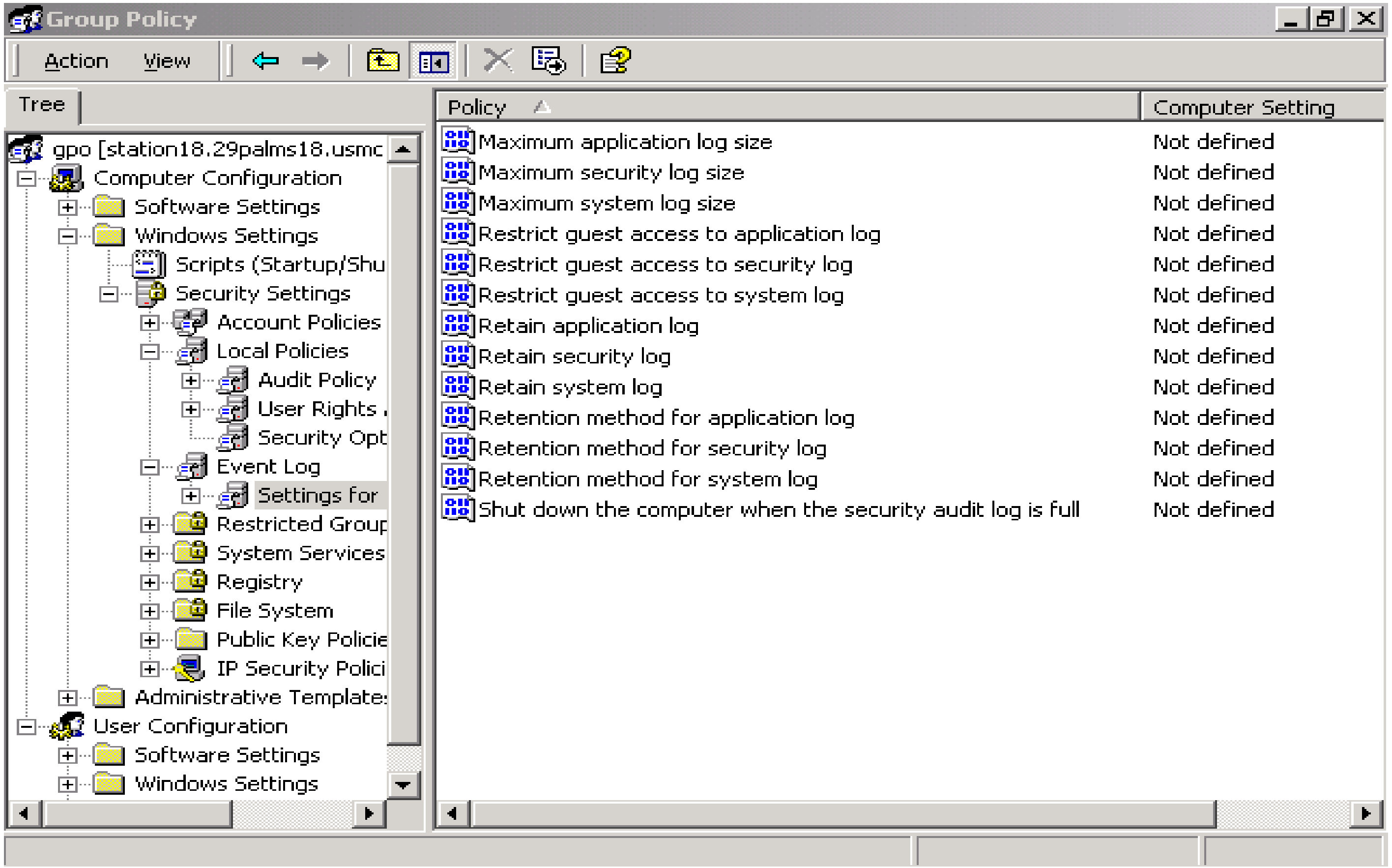


- gpo [station18.29palms18.usmc.mil]
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Scripts (Startup/Shutdo
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Ass
          - Security Option:
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Public Key Policies
        - IP Security Policies
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Policy	Computer Setting
Additional restrictions for anonymous connections	Not defined
Allow server operators to schedule tasks (domain controllers ...	Not defined
Allow system to be shut down without having to log on	Not defined
Allowed to eject removable NTFS media	Not defined
Amount of idle time required before disconnecting session	Not defined
Audit the access of global system objects	Not defined
Audit use of Backup and Restore privilege	Not defined
Automatically log off users when logon time expires	Not defined
Automatically log off users when logon time expires (local)	Not defined
Clear virtual memory pagefile when system shuts down	Not defined
Digitally sign client communication (always)	Not defined
Digitally sign client communication (when possible)	Not defined
Digitally sign server communication (always)	Not defined
Digitally sign server communication (when possible)	Not defined
Disable CTRL+ALT+DEL requirement for logon	Not defined
Do not display last user name in logon screen	Not defined
LAN Manager Authentication Level	Not defined
Message text for users attempting to log on	Not defined
Message title for users attempting to log on	Not defined
Number of previous logons to cache (in case domain controll...	Not defined
Prevent system maintenance of computer account password	Not defined
Prevent users from installing printer drivers	Not defined

CC Event Log Settings

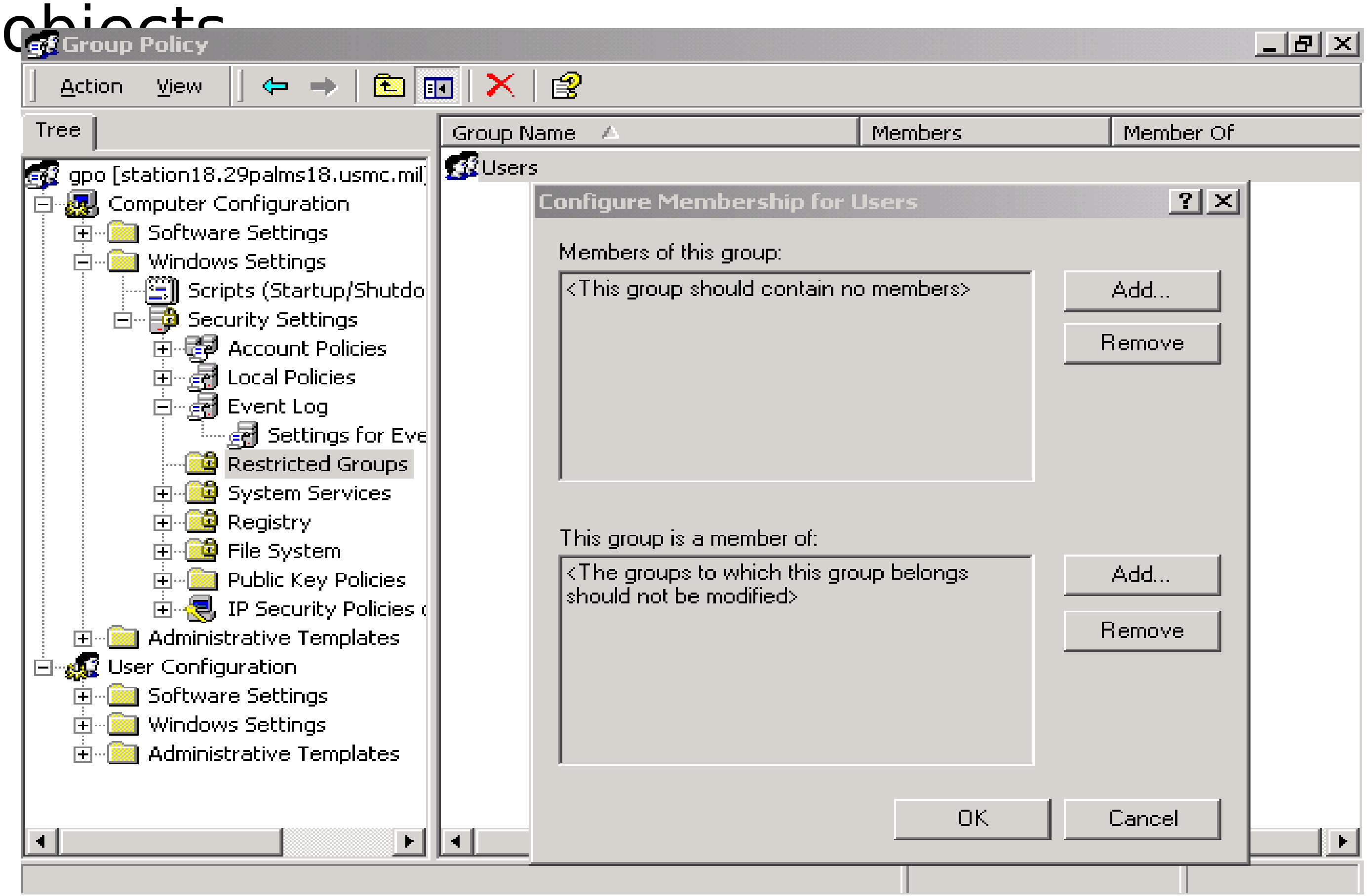
- Settings for Application, Security & System event logs in Event Viewer



Policy	Computer Setting
Maximum application log size	Not defined
Maximum security log size	Not defined
Maximum system log size	Not defined
Restrict guest access to application log	Not defined
Restrict guest access to security log	Not defined
Restrict guest access to system log	Not defined
Retain application log	Not defined
Retain security log	Not defined
Retain system log	Not defined
Retention method for application log	Not defined
Retention method for security log	Not defined
Retention method for system log	Not defined
Shut down the computer when the security audit log is full	Not defined

CC Restricted Groups

- Membership of group is restricted to certain objects



Members of this group:

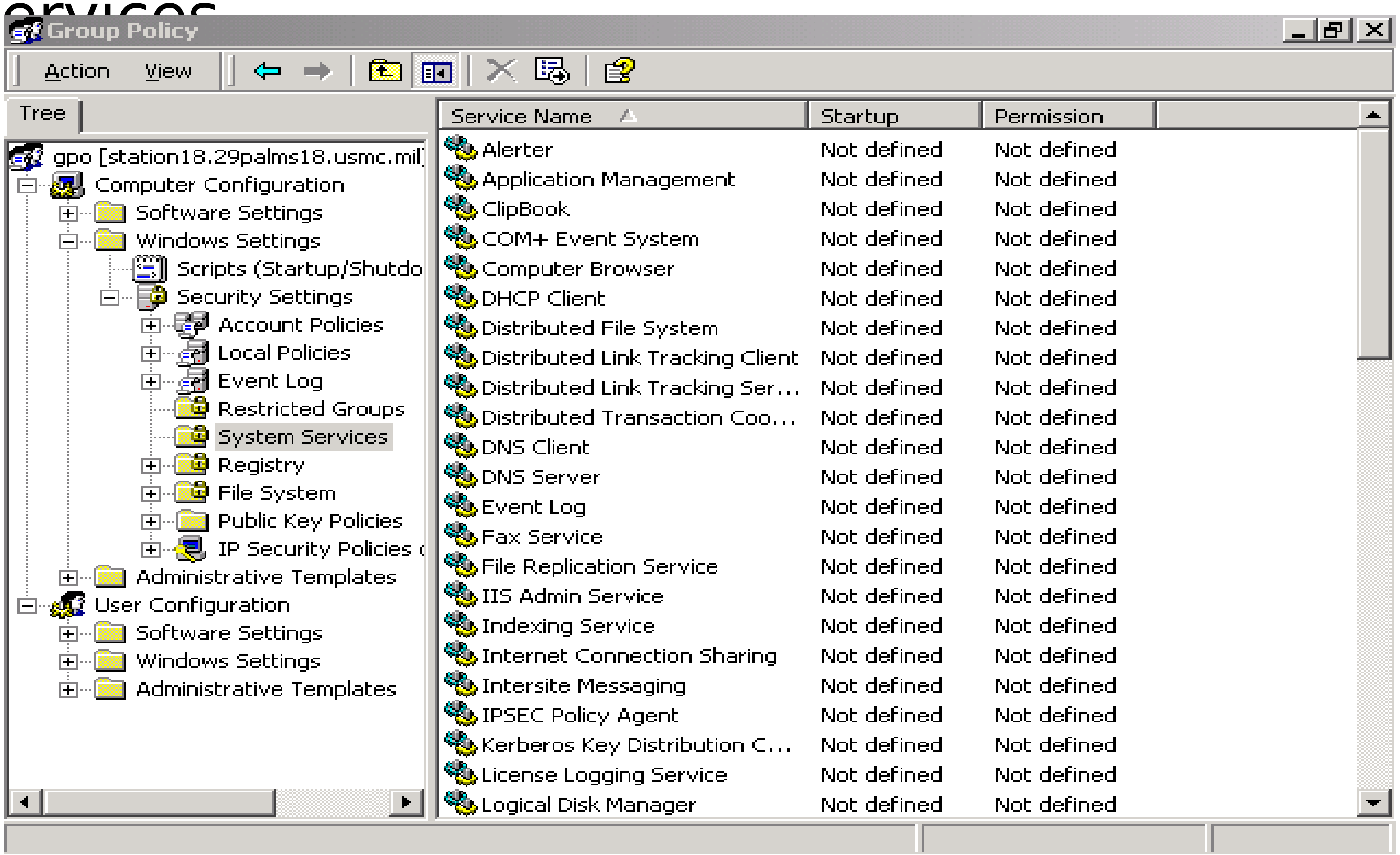
<This group should contain no members>

This group is a member of:

<The groups to which this group belongs should not be modified>

CC System Services

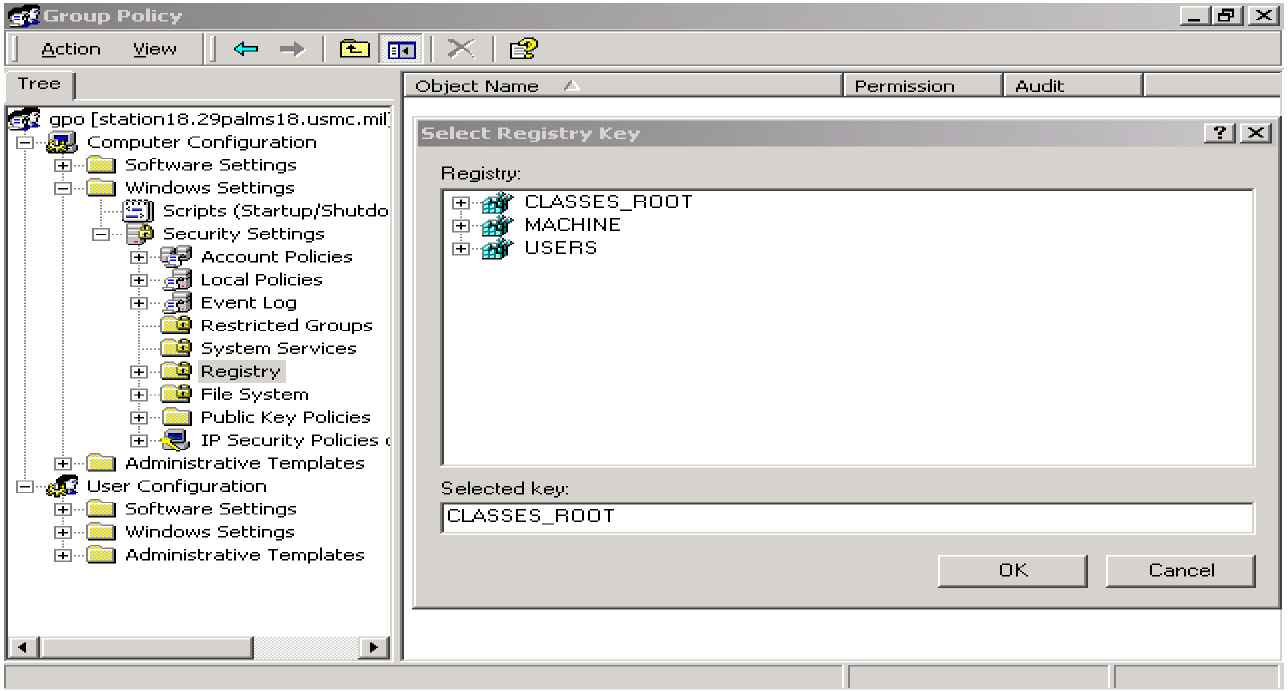
- Startup mode & security options for system services



Service Name	Startup	Permission
Alerter	Not defined	Not defined
Application Management	Not defined	Not defined
ClipBook	Not defined	Not defined
COM+ Event System	Not defined	Not defined
Computer Browser	Not defined	Not defined
DHCP Client	Not defined	Not defined
Distributed File System	Not defined	Not defined
Distributed Link Tracking Client	Not defined	Not defined
Distributed Link Tracking Ser...	Not defined	Not defined
Distributed Transaction Coo...	Not defined	Not defined
DNS Client	Not defined	Not defined
DNS Server	Not defined	Not defined
Event Log	Not defined	Not defined
Fax Service	Not defined	Not defined
File Replication Service	Not defined	Not defined
IIS Admin Service	Not defined	Not defined
Indexing Service	Not defined	Not defined
Internet Connection Sharing	Not defined	Not defined
Intersite Messaging	Not defined	Not defined
IPSEC Policy Agent	Not defined	Not defined
Kerberos Key Distribution C...	Not defined	Not defined
License Logging Service	Not defined	Not defined
Logical Disk Manager	Not defined	Not defined

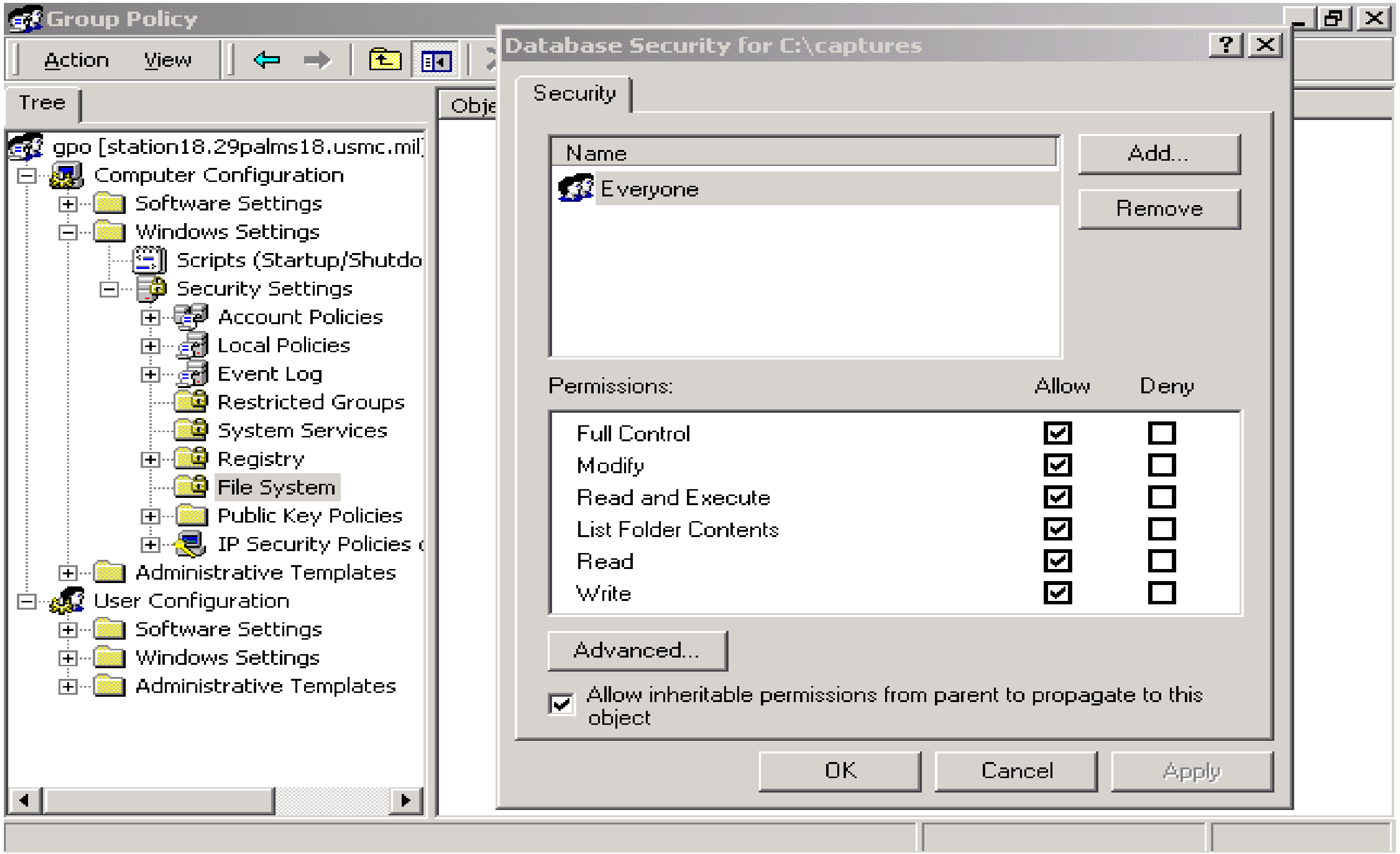
CC Registry

- Configures security settings for registry keys
  - Registry settings governing behavior / appearance of desktop
  - Written to HKEY_CURRENT_USER and HKEY_LOCAL_MACHINE



CC File System

- Settings for file-system objects including permissions, audit, & ownership



Database Security for C:\captures

Security

Name
Everyone

Add... Remove

Permissions:	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read and Execute	☑	□
List Folder Contents	☑	□
Read	☑	□
Write	☑	□

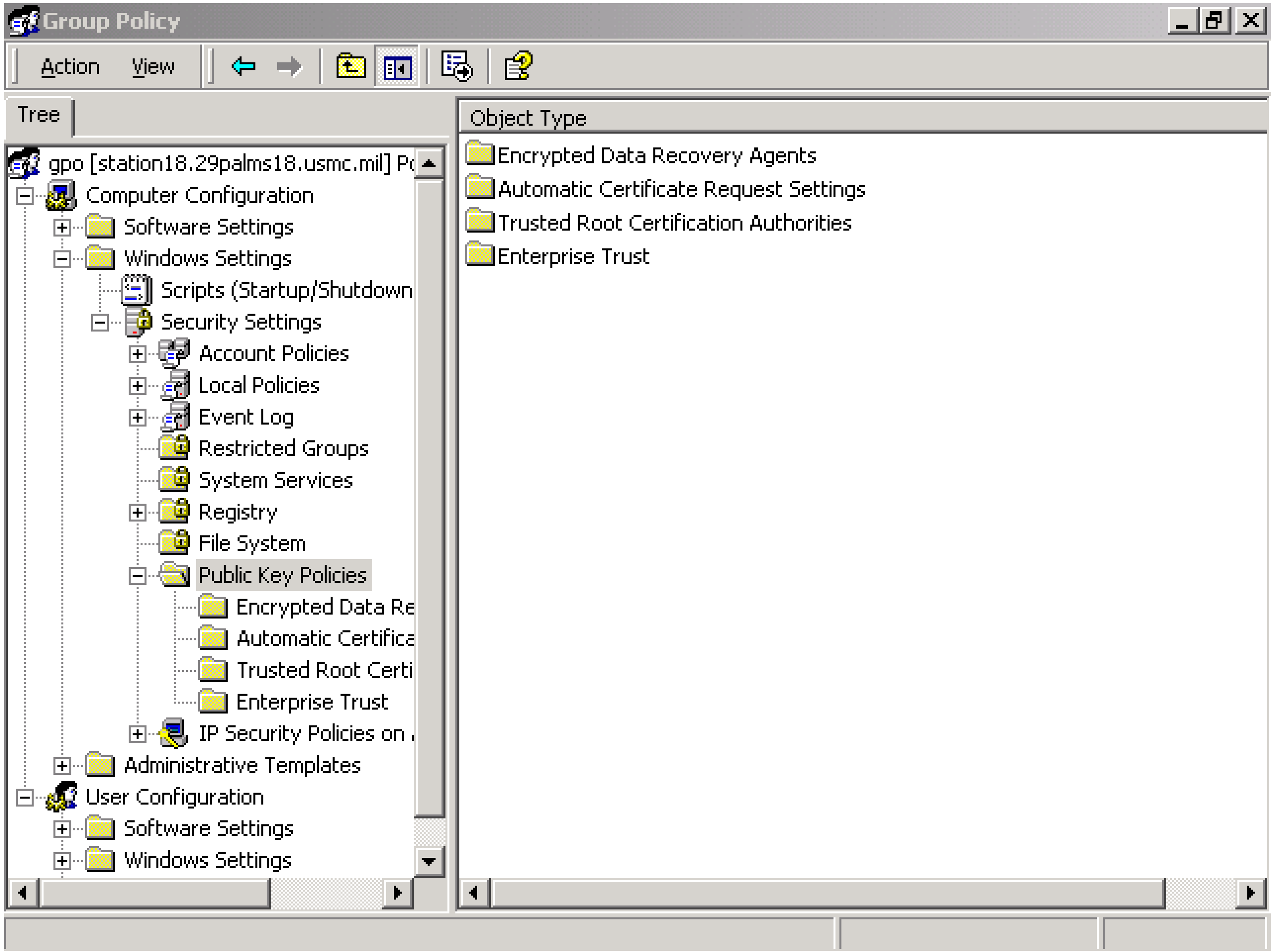
Advanced...

☑ Allow inheritable permissions from parent to propagate to this object

OK Cancel Apply

CC Public Key Policies -- Certificates

- Set public / private key access for encryption



Object Type

Encrypted Data Recovery Agents

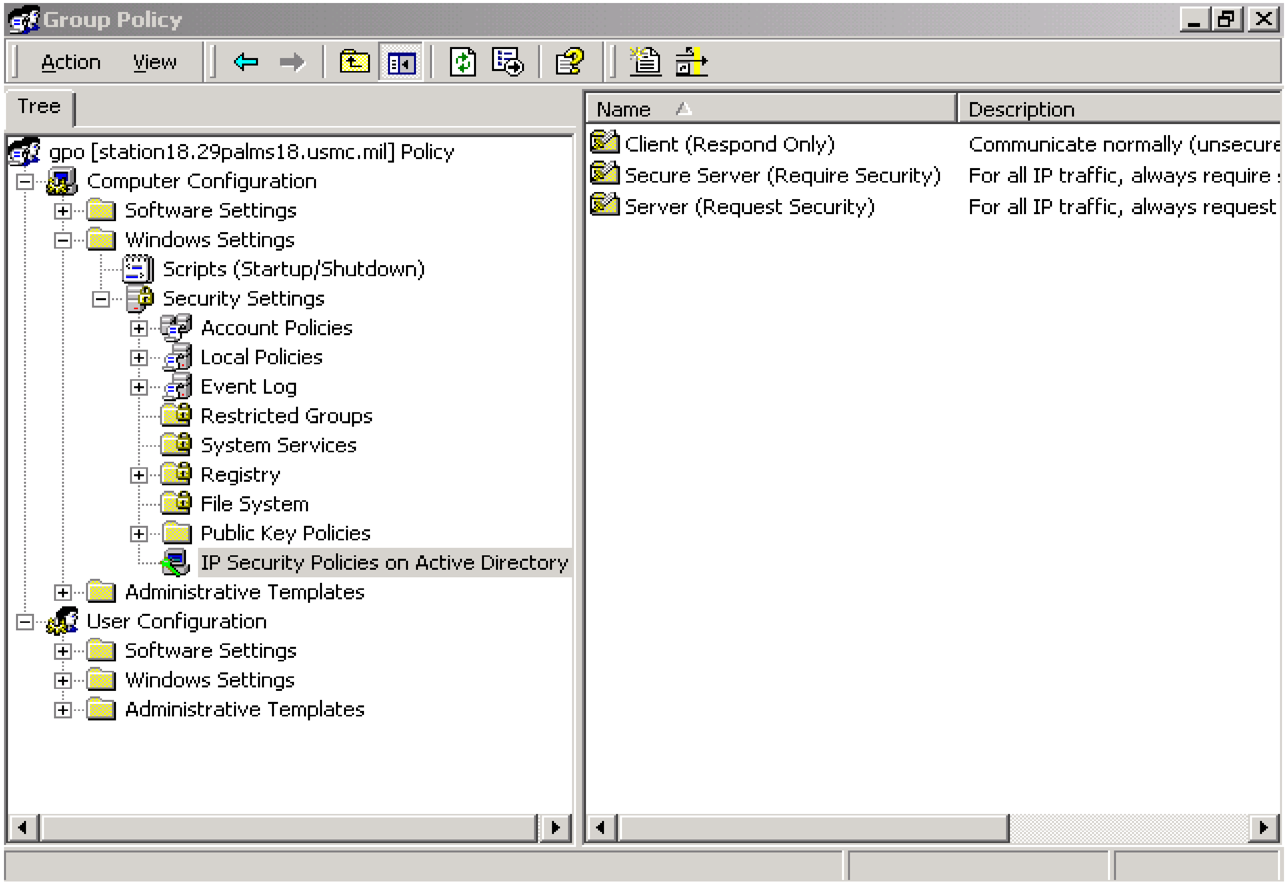
Automatic Certificate Request Settings

Trusted Root Certification Authorities

Enterprise Trust

CC IP Security

- Configure IP security (IPSec) policy

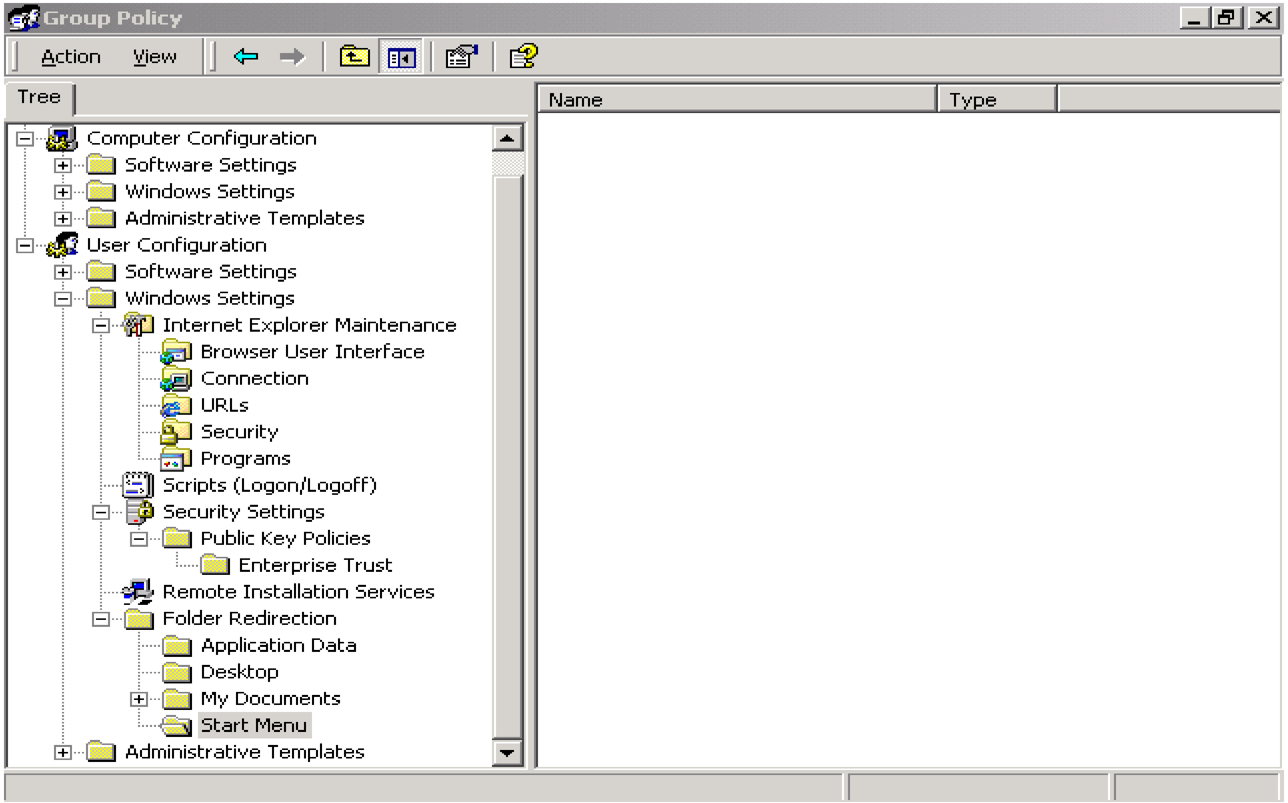


gpo [station18.29palms18.usmc.mil] Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
    - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
      - Local Policies
      - Event Log
      - Restricted Groups
      - System Services
      - Registry
      - File System
      - Public Key Policies
      - IP Security Policies on Active Directory
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

Name	Description
Client (Respond Only)	Communicate normally (unsecure
Secure Server (Require Security)	For all IP traffic, always require :
Server (Request Security)	For all IP traffic, always request

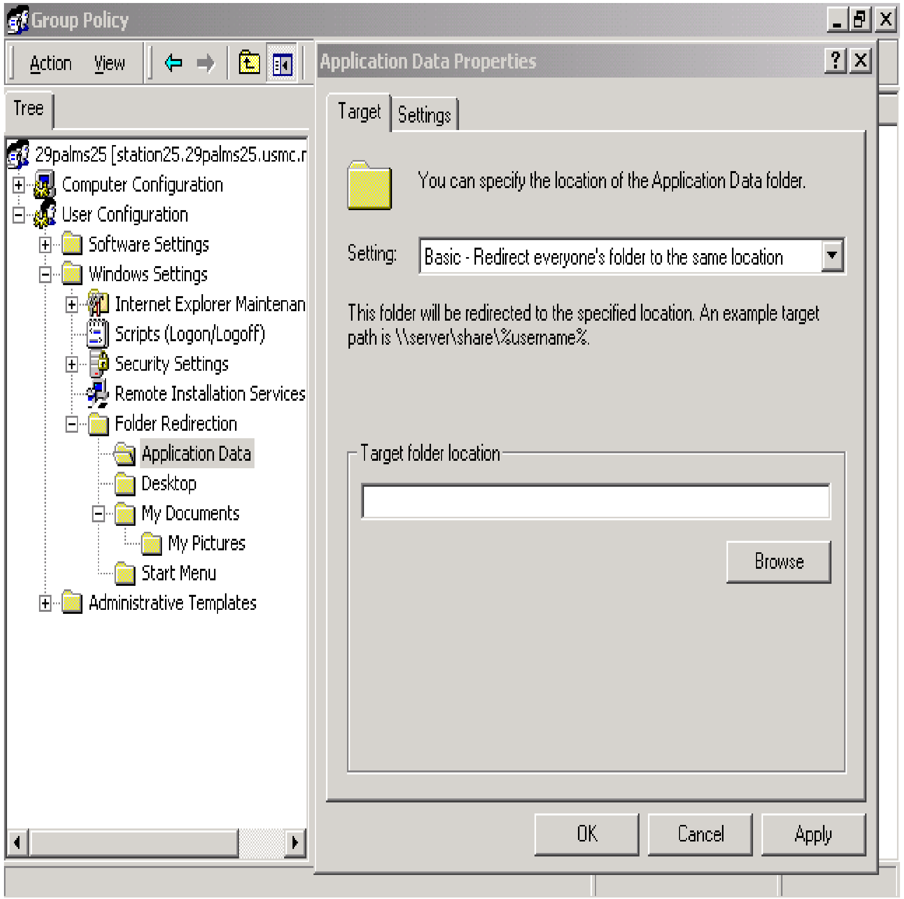
UC Windows Settings

- Internet Explorer Maintenance, Security Settings, RIS, Folder Redirection



UC -- Folder Redirection Basic

- Redirect special folders from the user profile location to an alternate location for all users



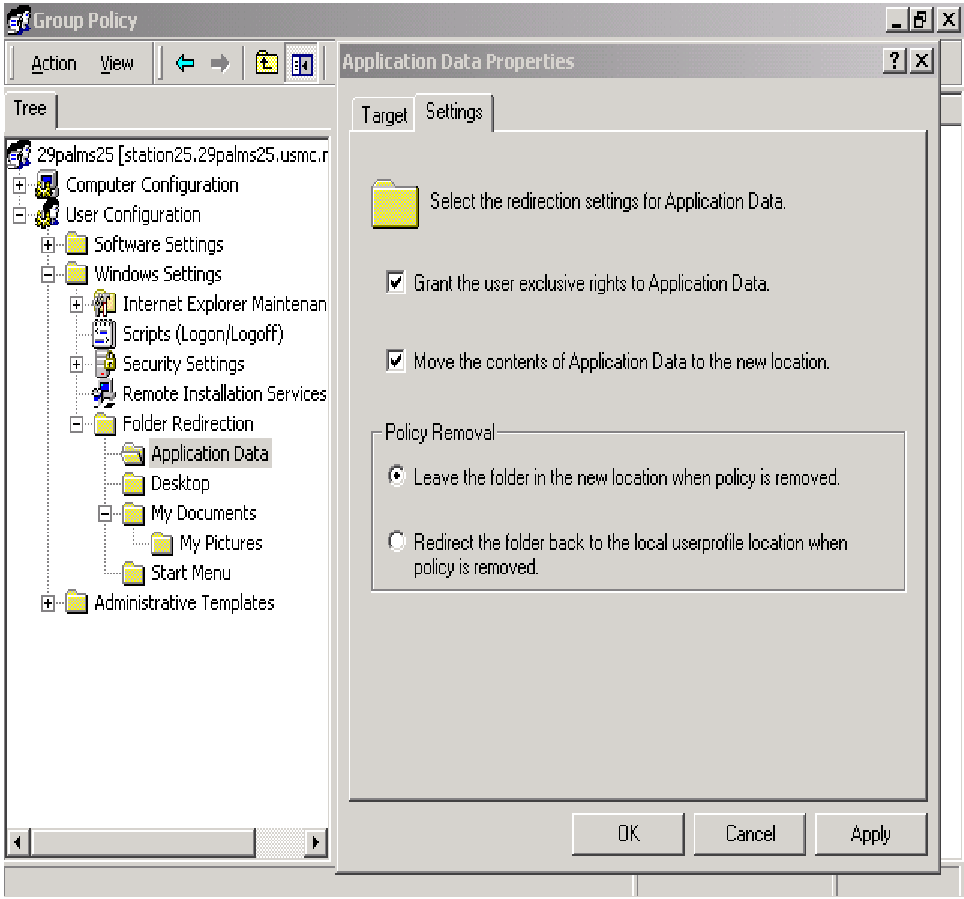
Application Data Properties — Target

You can specify the location of the Application Data folder.

Setting: Basic - Redirect everyone's folder to the same location

This folder will be redirected to the specified location. An example target path is \\server\share\%username%.

Target folder location



Application Data Properties — Settings

Select the redirection settings for Application Data.

☑ Grant the user exclusive rights to Application Data.

☑ Move the contents of Application Data to the new location.

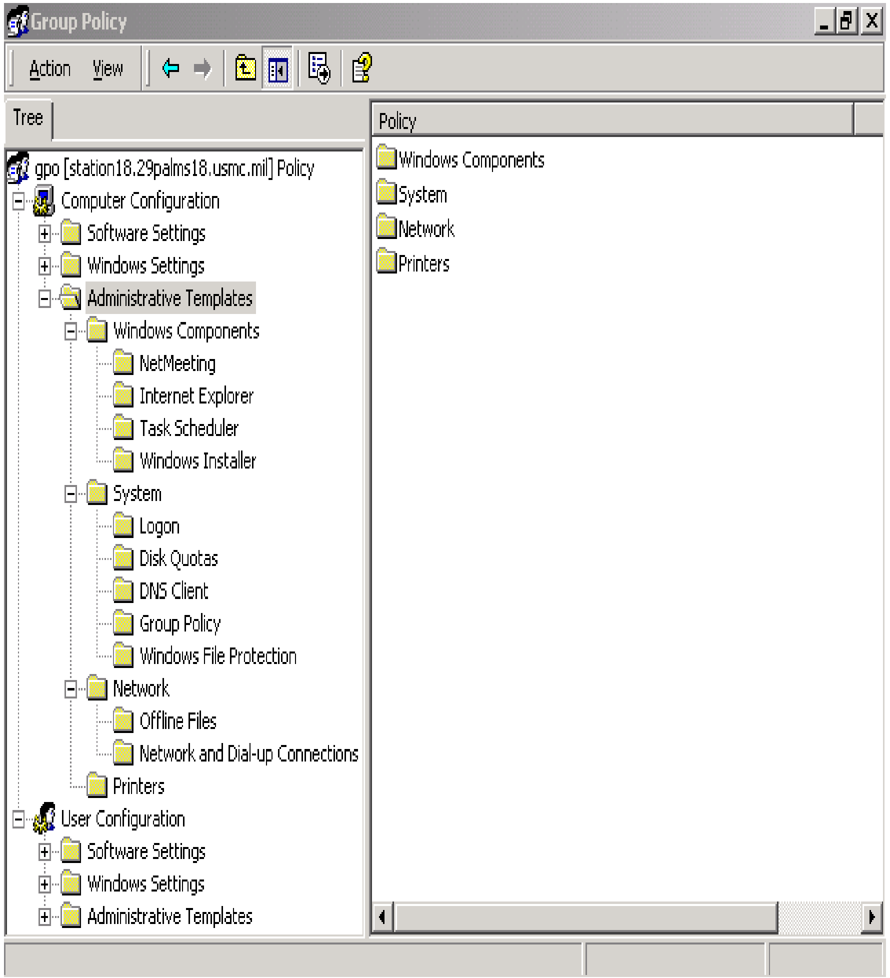
Policy Removal

● Leave the folder in the new location when policy is removed.

○ Redirect the folder back to the local userprofile location when policy is removed.

CC Administrative Templates

- Several sections to affect settings that govern behavior and appearance of desktop
- Windows Components varied with different options to manage

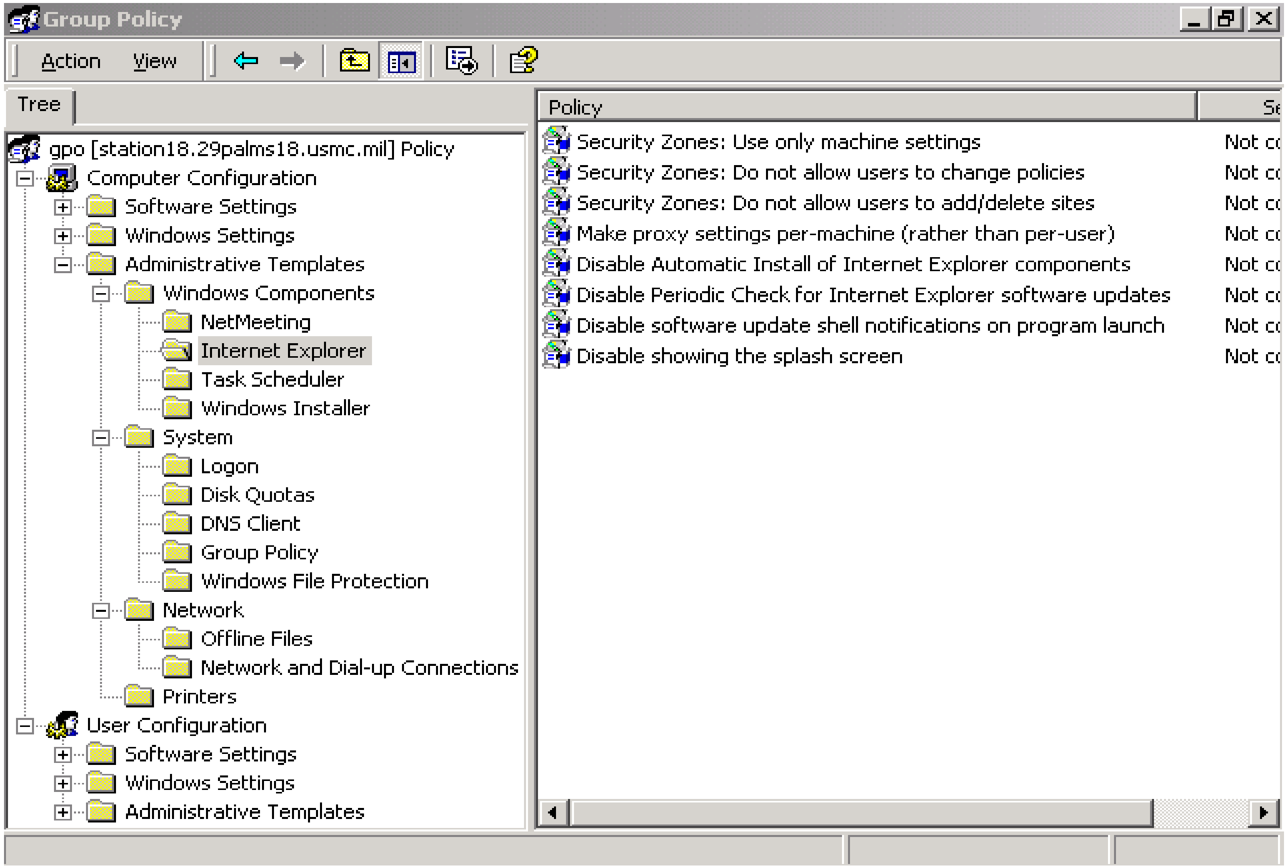


gpo [station18.29palms18.usmc.mil] Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Windows Components
      - NetMeeting
      - Internet Explorer
      - Task Scheduler
      - Windows Installer
    - System
      - Logon
      - Disk Quotas
      - DNS Client
      - Group Policy
      - Windows File Protection
    - Network
      - Offline Files
      - Network and Dial-up Connections
    - Printers
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

Windows Components
System
Network
Printers

CC Internet Explorer

- Double-click any options to find an explanation of enabling the policy

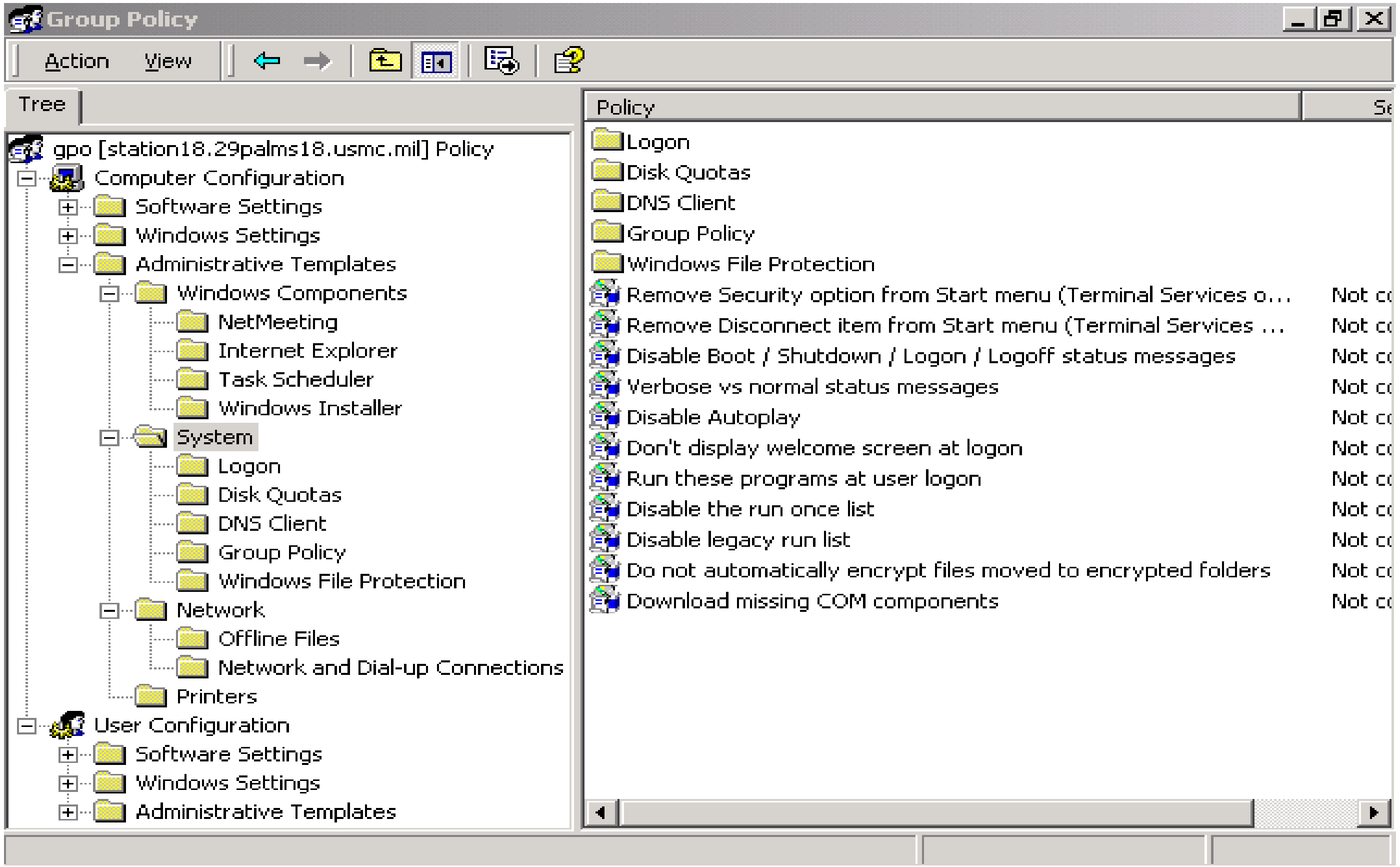


```
gpo [station18.29palms18.usmc.mil] Policy
  Computer Configuration
    Software Settings
    Windows Settings
    Administrative Templates
      Windows Components
        NetMeeting
        Internet Explorer
        Task Scheduler
        Windows Installer
      System
        Logon
        Disk Quotas
        DNS Client
        Group Policy
        Windows File Protection
      Network
        Offline Files
        Network and Dial-up Connections
      Printers
  User Configuration
    Software Settings
    Windows Settings
    Administrative Templates
```

Policy	Se
Security Zones: Use only machine settings	Not c
Security Zones: Do not allow users to change policies	Not c
Security Zones: Do not allow users to add/delete sites	Not c
Make proxy settings per-machine (rather than per-user)	Not c
Disable Automatic Install of Internet Explorer components	Not c
Disable Periodic Check for Internet Explorer software updates	Not c
Disable software update shell notifications on program launch	Not c
Disable showing the splash screen	Not c

CC System

- Affects Logon, Disk Quotas, DNS Client, Group Policy and Windows File Protection

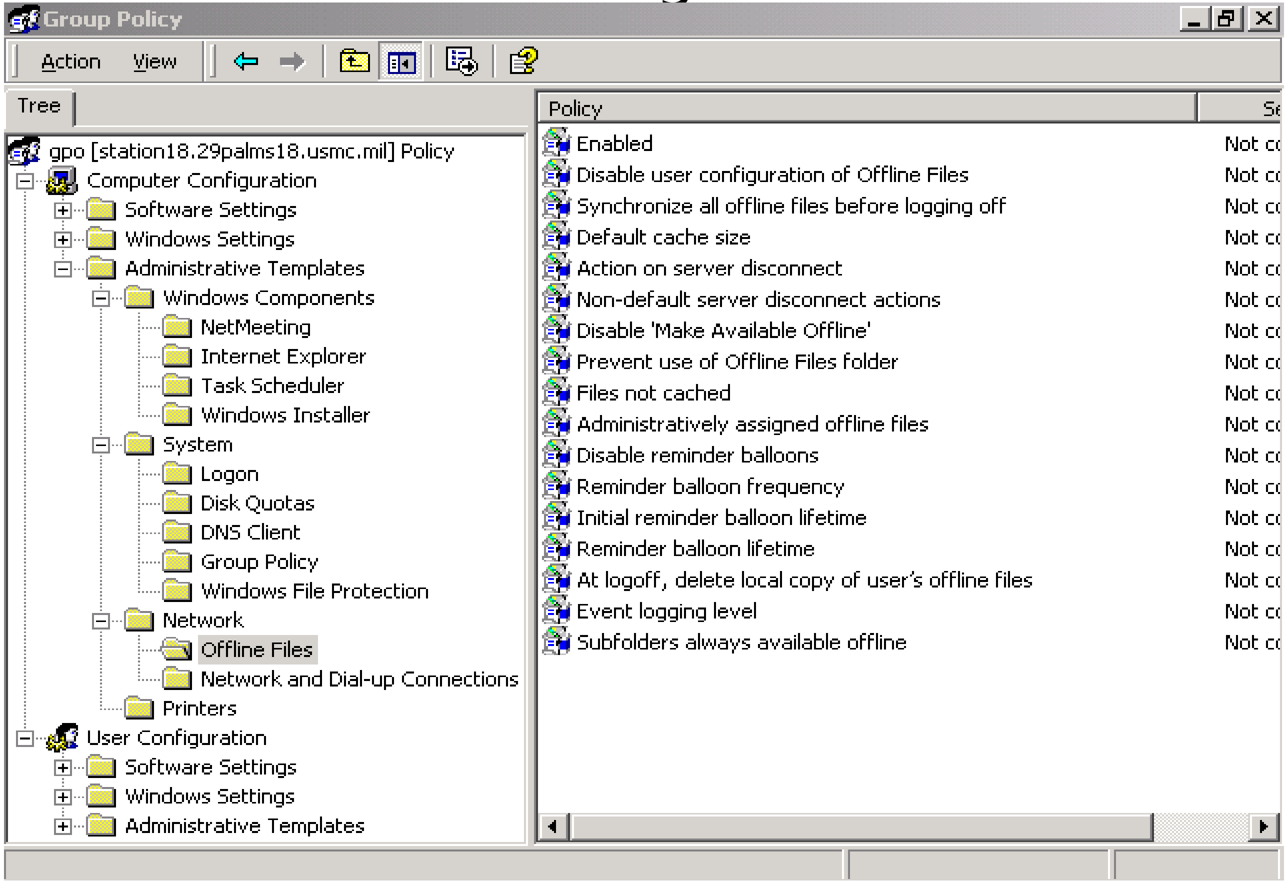


- gpo [station18.29palms18.usmc.mil] Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Windows Components
        - NetMeeting
        - Internet Explorer
        - Task Scheduler
        - Windows Installer
      - System
        - Logon
        - Disk Quotas
        - DNS Client
        - Group Policy
        - Windows File Protection
      - Network
        - Offline Files
        - Network and Dial-up Connections
      - Printers
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Policy	Se
Logon	
Disk Quotas	
DNS Client	
Group Policy	
Windows File Protection	
Remove Security option from Start menu (Terminal Services o...	Not c
Remove Disconnect item from Start menu (Terminal Services ...	Not c
Disable Boot / Shutdown / Logon / Logoff status messages	Not c
Verbose vs normal status messages	Not c
Disable Autoplay	Not c
Don't display welcome screen at logon	Not c
Run these programs at user logon	Not c
Disable the run once list	Not c
Disable legacy run list	Not c
Do not automatically encrypt files moved to encrypted folders	Not c
Download missing COM components	Not c

CC Offline Files

- For laptop users as part of the domain working on files without having to be connected

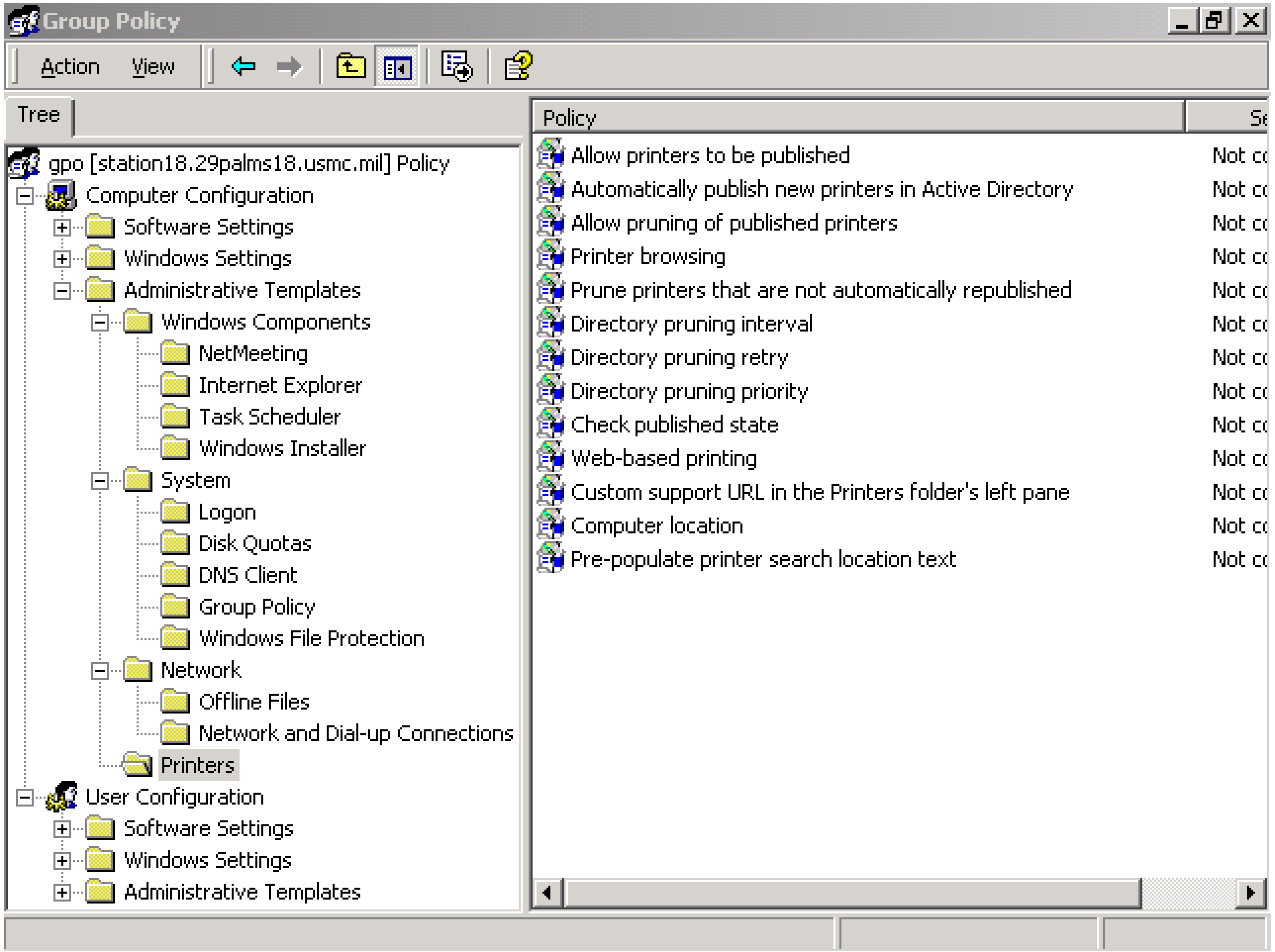


- gpo [station18.29palms18.usmc.mil] Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Windows Components
        - NetMeeting
        - Internet Explorer
        - Task Scheduler
        - Windows Installer
      - System
        - Logon
        - Disk Quotas
        - DNS Client
        - Group Policy
        - Windows File Protection
      - Network
        - Offline Files
        - Network and Dial-up Connections
      - Printers
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Policy	Se
Enabled	Not c
Disable user configuration of Offline Files	Not c
Synchronize all offline files before logging off	Not c
Default cache size	Not c
Action on server disconnect	Not c
Non-default server disconnect actions	Not c
Disable 'Make Available Offline'	Not c
Prevent use of Offline Files folder	Not c
Files not cached	Not c
Administratively assigned offline files	Not c
Disable reminder balloons	Not c
Reminder balloon frequency	Not c
Initial reminder balloon lifetime	Not c
Reminder balloon lifetime	Not c
At logoff, delete local copy of user's offline files	Not c
Event logging level	Not c
Subfolders always available offline	Not c

CC Printers

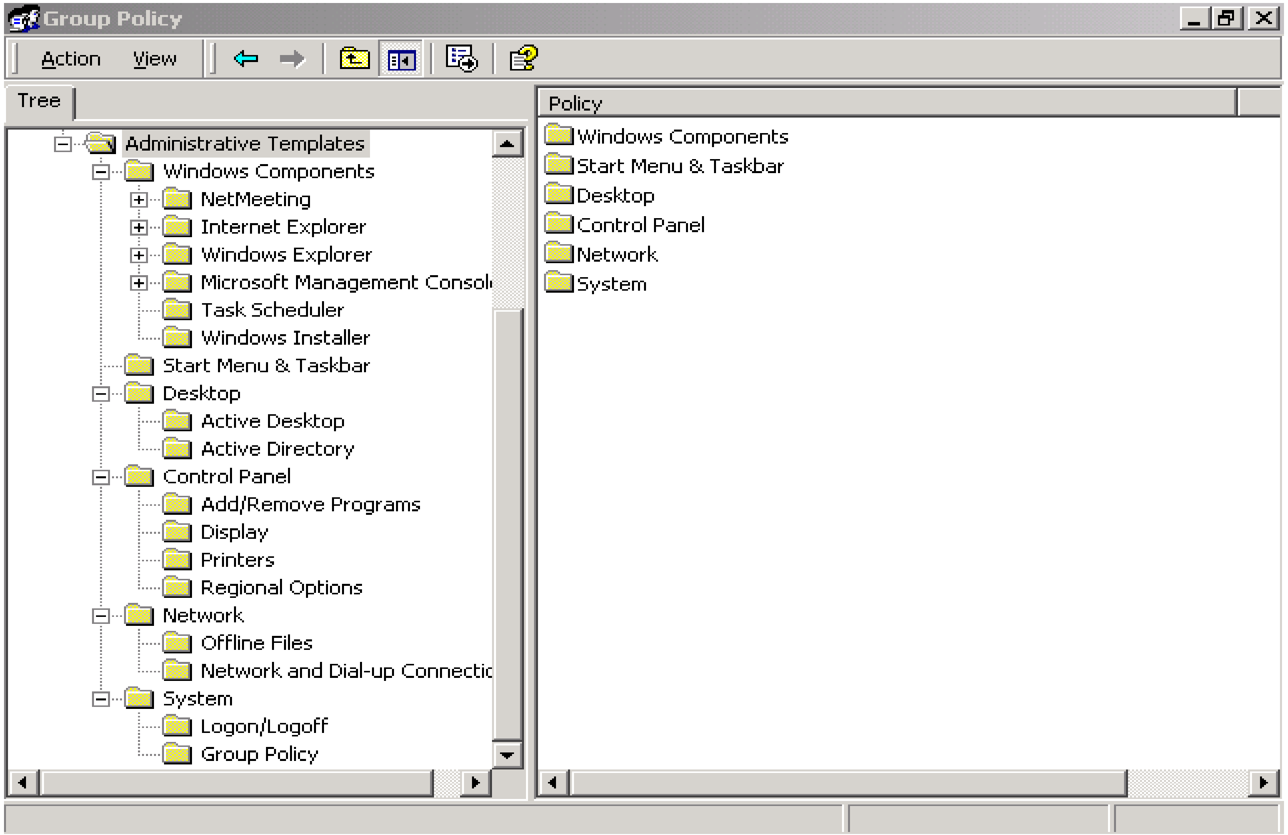
- Security options for printers in the Domain/OU



Policy	Se
Allow printers to be published	Not co
Automatically publish new printers in Active Directory	Not co
Allow pruning of published printers	Not co
Printer browsing	Not co
Prune printers that are not automatically republished	Not co
Directory pruning interval	Not co
Directory pruning retry	Not co
Directory pruning priority	Not co
Check published state	Not co
Web-based printing	Not co
Custom support URL in the Printers folder's left pane	Not co
Computer location	Not co
Pre-populate printer search location text	Not co

UC Administrative Templates

- Windows Components, Start Menu & Taskbar, Desktop, Control Panel, Network and System

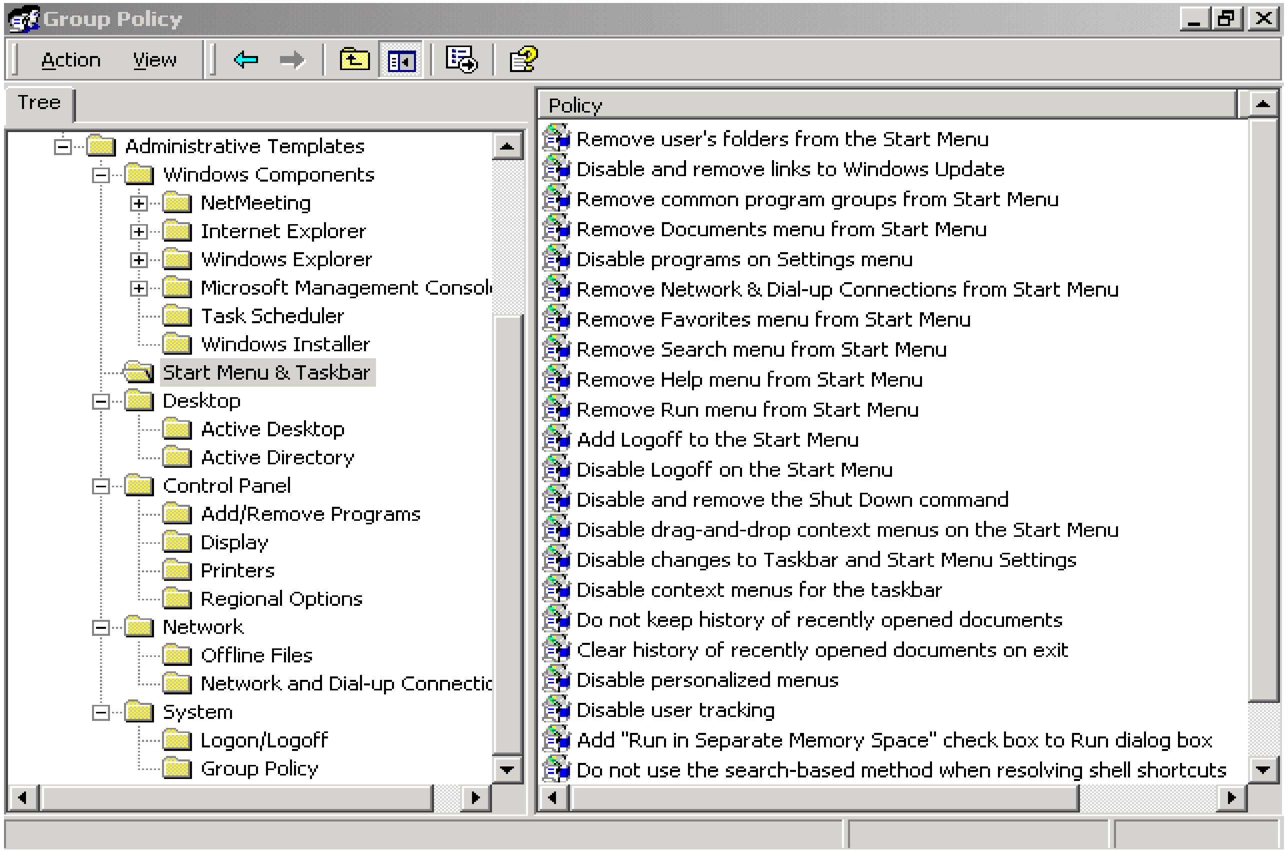


- Administrative Templates
  - Windows Components
    - NetMeeting
    - Internet Explorer
    - Windows Explorer
    - Microsoft Management Consol
    - Task Scheduler
    - Windows Installer
  - Start Menu & Taskbar
  - Desktop
    - Active Desktop
    - Active Directory
  - Control Panel
    - Add/Remove Programs
    - Display
    - Printers
    - Regional Options
  - Network
    - Offline Files
    - Network and Dial-up Connectic
  - System
    - Logon/Logoff
    - Group Policy

Windows Components
Start Menu & Taskbar
Desktop
Control Panel
Network
System

UC Start Menu & Taskbar

- Policies like removing and disabling options from the start menu or taskbar are available

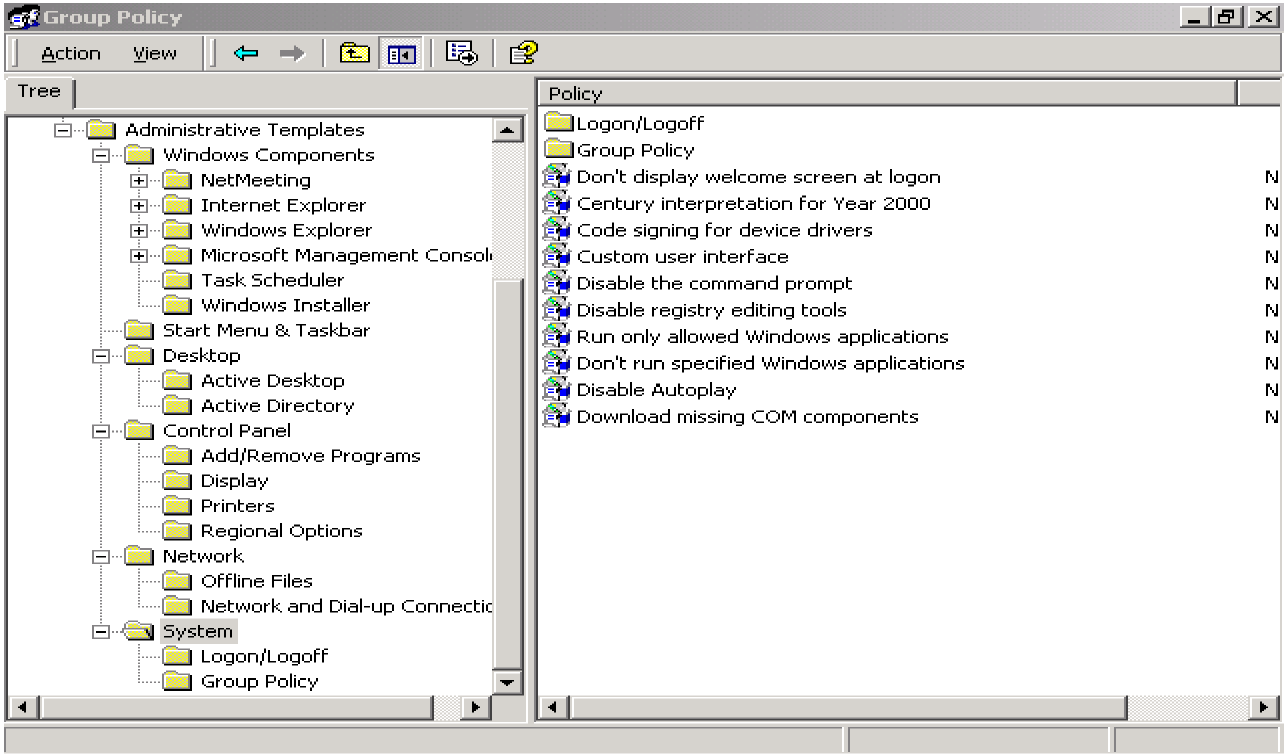


Policy

- Remove user's folders from the Start Menu
- Disable and remove links to Windows Update
- Remove common program groups from Start Menu
- Remove Documents menu from Start Menu
- Disable programs on Settings menu
- Remove Network & Dial-up Connections from Start Menu
- Remove Favorites menu from Start Menu
- Remove Search menu from Start Menu
- Remove Help menu from Start Menu
- Remove Run menu from Start Menu
- Add Logoff to the Start Menu
- Disable Logoff on the Start Menu
- Disable and remove the Shut Down command
- Disable drag-and-drop context menus on the Start Menu
- Disable changes to Taskbar and Start Menu Settings
- Disable context menus for the taskbar
- Do not keep history of recently opened documents
- Clear history of recently opened documents on exit
- Disable personalized menus
- Disable user tracking
- Add "Run in Separate Memory Space" check box to Run dialog box
- Do not use the search-based method when resolving shell shortcuts

UC Desktop / Control Panel / Network

- Desktop -- Active Desktop / Directory
- Control Panel -- Lock available options
- Network -- Offline files / Network & Dial-up

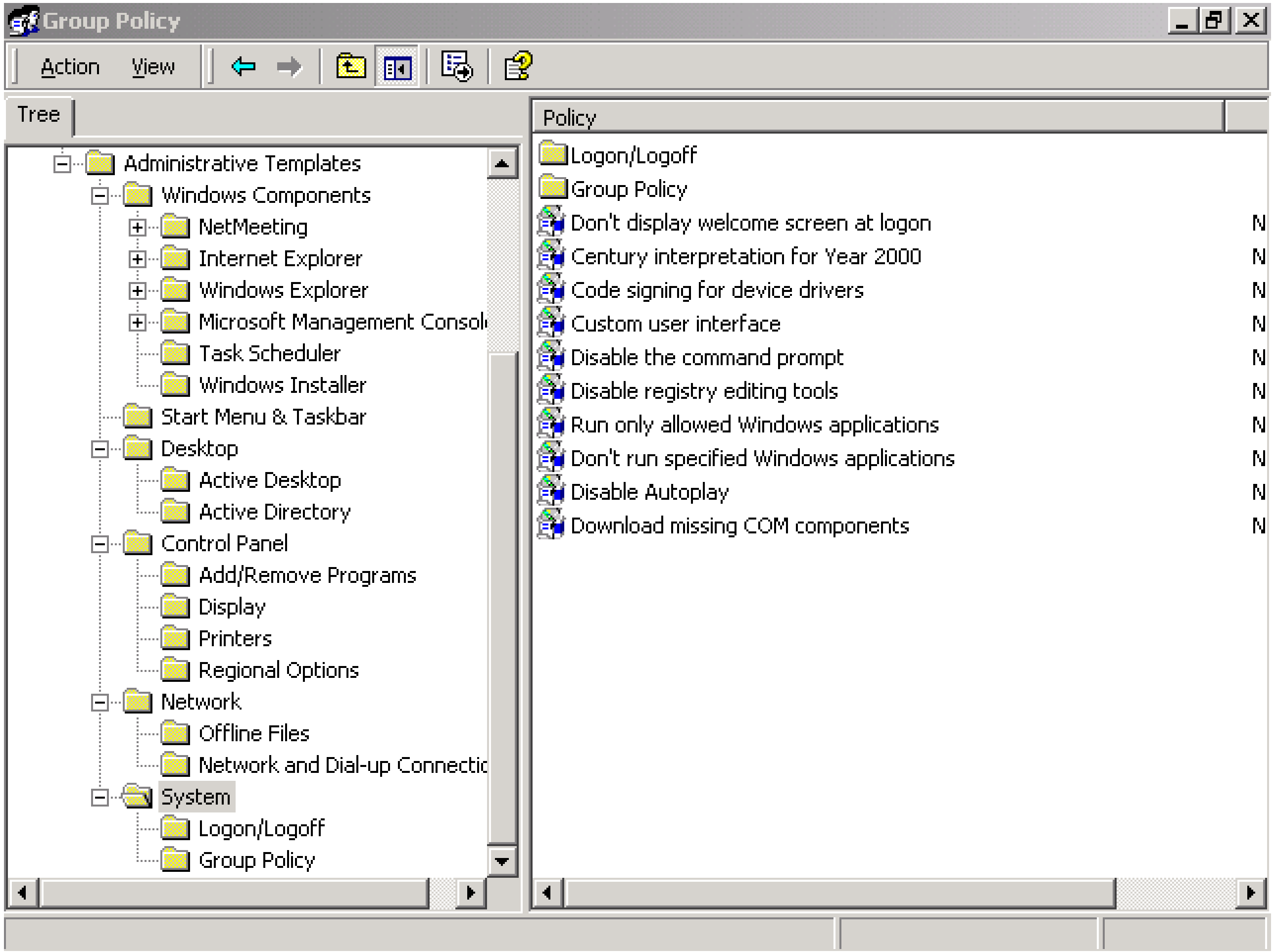


```
Administrative Templates
    Windows Components
        NetMeeting
        Internet Explorer
        Windows Explorer
        Microsoft Management Consol
        Task Scheduler
        Windows Installer
    Start Menu & Taskbar
    Desktop
        Active Desktop
        Active Directory
    Control Panel
        Add/Remove Programs
        Display
        Printers
        Regional Options
    Network
        Offline Files
        Network and Dial-up Connectic
    System
        Logon/Logoff
        Group Policy
```

```
Logon/Logoff
Group Policy
Don't display welcome screen at logon          N
Century interpretation for Year 2000           N
Code signing for device drivers                N
Custom user interface                          N
Disable the command prompt                     N
Disable registry editing tools                 N
Run only allowed Windows applications          N
Don't run specified Windows applications       N
Disable Autoplay                               N
Download missing COM components                N
```

UC System

- Disable options, Logon/off, Group Policy



- Administrative Templates
  - Windows Components
    - NetMeeting
    - Internet Explorer
    - Windows Explorer
    - Microsoft Management Consol
    - Task Scheduler
    - Windows Installer
  - Start Menu & Taskbar
  - Desktop
    - Active Desktop
    - Active Directory
  - Control Panel
    - Add/Remove Programs
    - Display
    - Printers
    - Regional Options
  - Network
    - Offline Files
    - Network and Dial-up Connectic
  - System
    - Logon/Logoff
    - Group Policy

Policy	
Logon/Logoff	
Group Policy	
Don't display welcome screen at logon	N
Century interpretation for Year 2000	N
Code signing for device drivers	N
Custom user interface	N
Disable the command prompt	N
Disable registry editing tools	N
Run only allowed Windows applications	N
Don't run specified Windows applications	N
Disable Autoplay	N
Download missing COM components	N

NT vs 2003 Policies

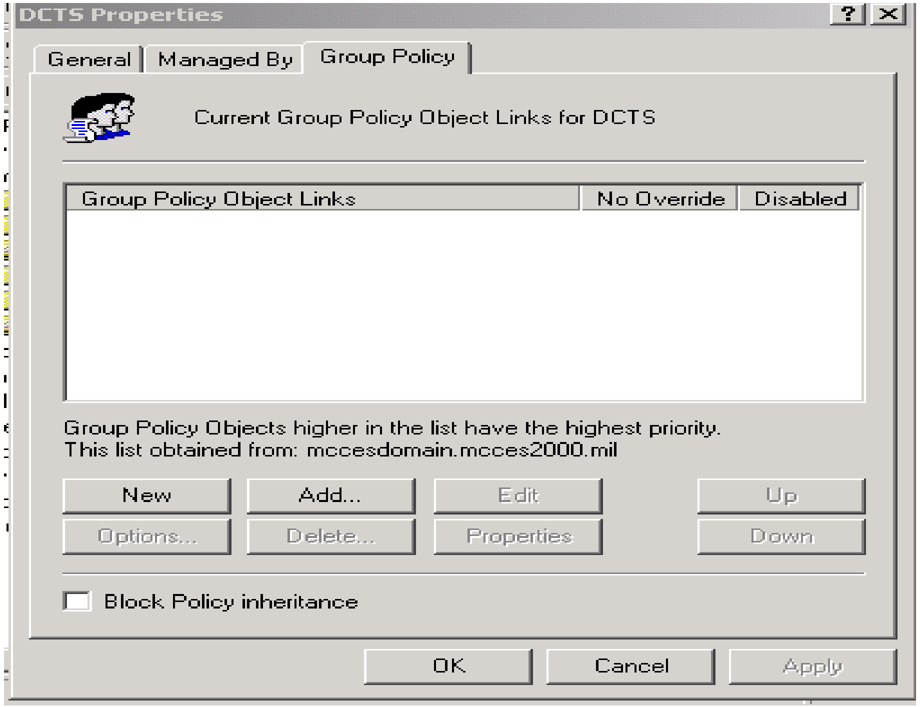
- Group policies created in Windows 2003 can NOT be applied to Windows 95/98/NT
- System Policy Editor policies can NOT be applied to Windows 2003
- If policy needs set for Windows 95/98/NT in a 2003 arena, use POLEDIT.EXE to create, but store CONFIG.POL or NTCONFIG.POL in the NETLOGON share for 2003 located in %systemroot%\SYSVOL\Sysvol\DomainName.com\Scripts

Managing Group Policy

- For domain or OU, use AD Users and Computers
- For site use AD Sites and Services
- Through either snap-in process is same
- For the Future
  - When and if XP clients start to come online, extended GPO options for Windows XP can be installed into the default Windows 2003 GPO options. See technet or search google.com for more information.

Managing Group Policy

- SELECT OBJECT -- Select the site, domain or OU object and open its properties
- Click Group Policy tab



Current Group Policy Object Links for DCTS

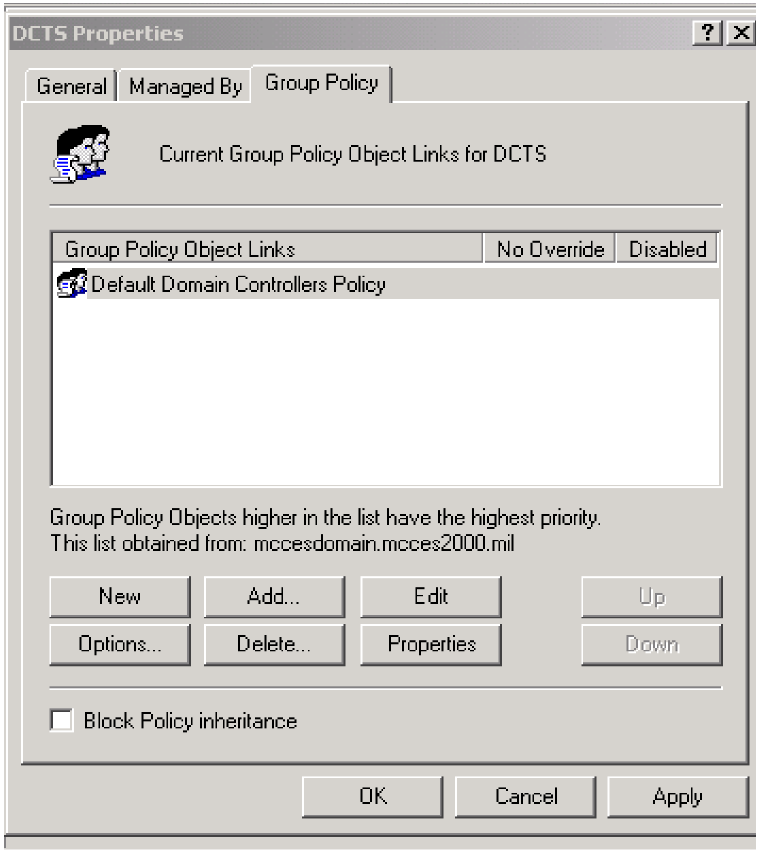
Group Policy Object Links	No Override	Disabled

Group Policy Objects higher in the list have the highest priority.
This list obtained from: mccesdomain.mcces2000.mil

☐ Block Policy inheritance

Managing Group Policy

- Click ADD an existing GPO click ADD & and select the appropriate GPO from All tab



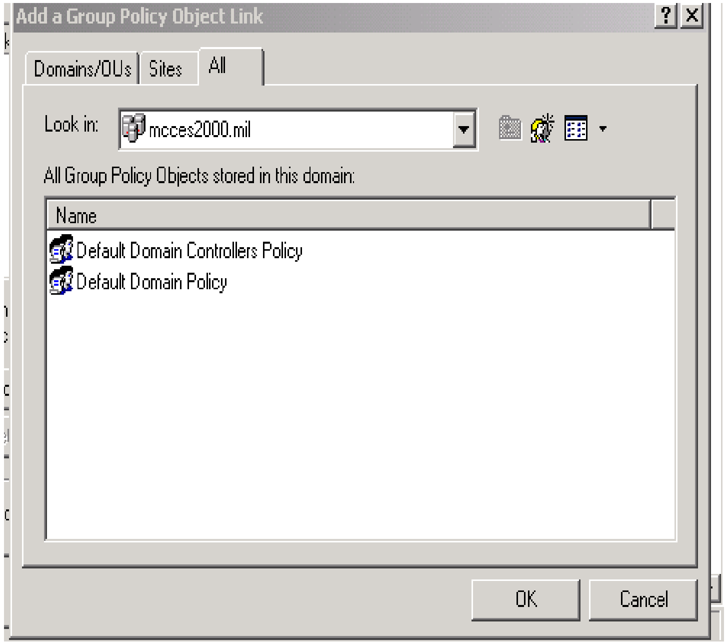
DCTS Properties

Current Group Policy Object Links for DCTS

Group Policy Object Links	No Override	Disabled
Default Domain Controllers Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: mccesdomain.mcces2000.mil

□ Block Policy inheritance



Add a Group Policy Object Link

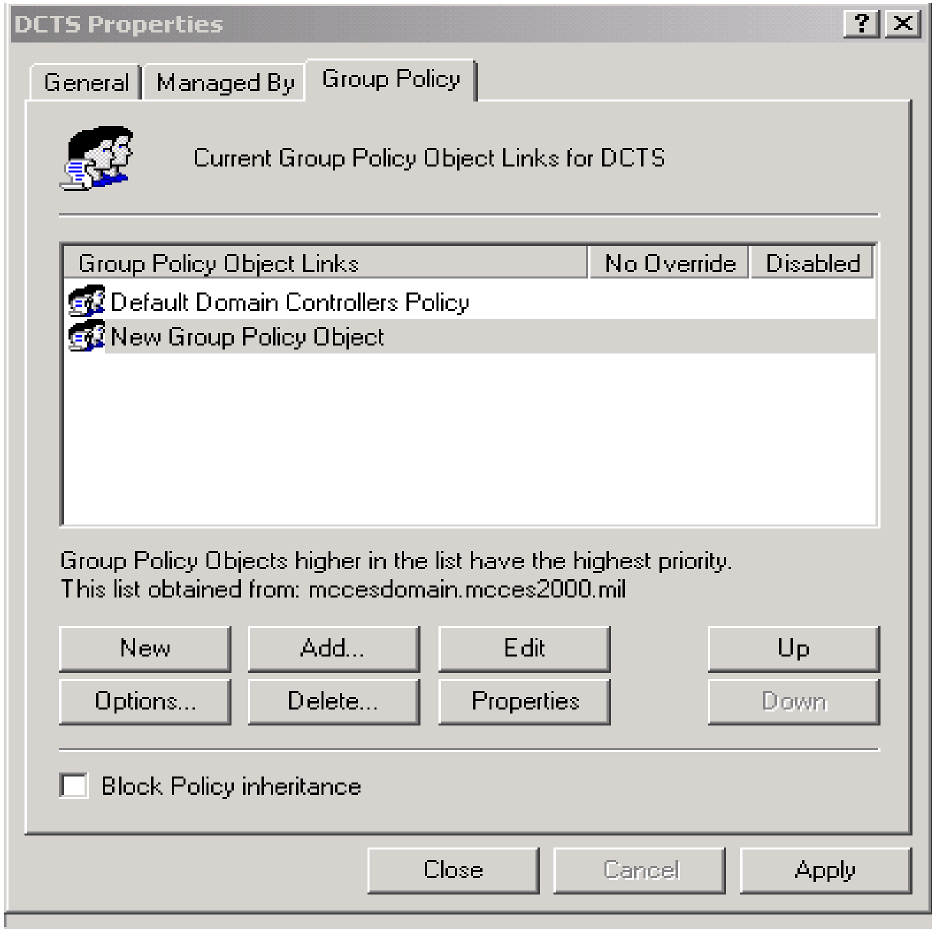
Look in: mcces2000.mil

All Group Policy Objects stored in this domain:

Name
Default Domain Controllers Policy
Default Domain Policy

Managing Group Policy

- Click NEW and enter a name for the object



DCTS Properties

Current Group Policy Object Links for DCTS

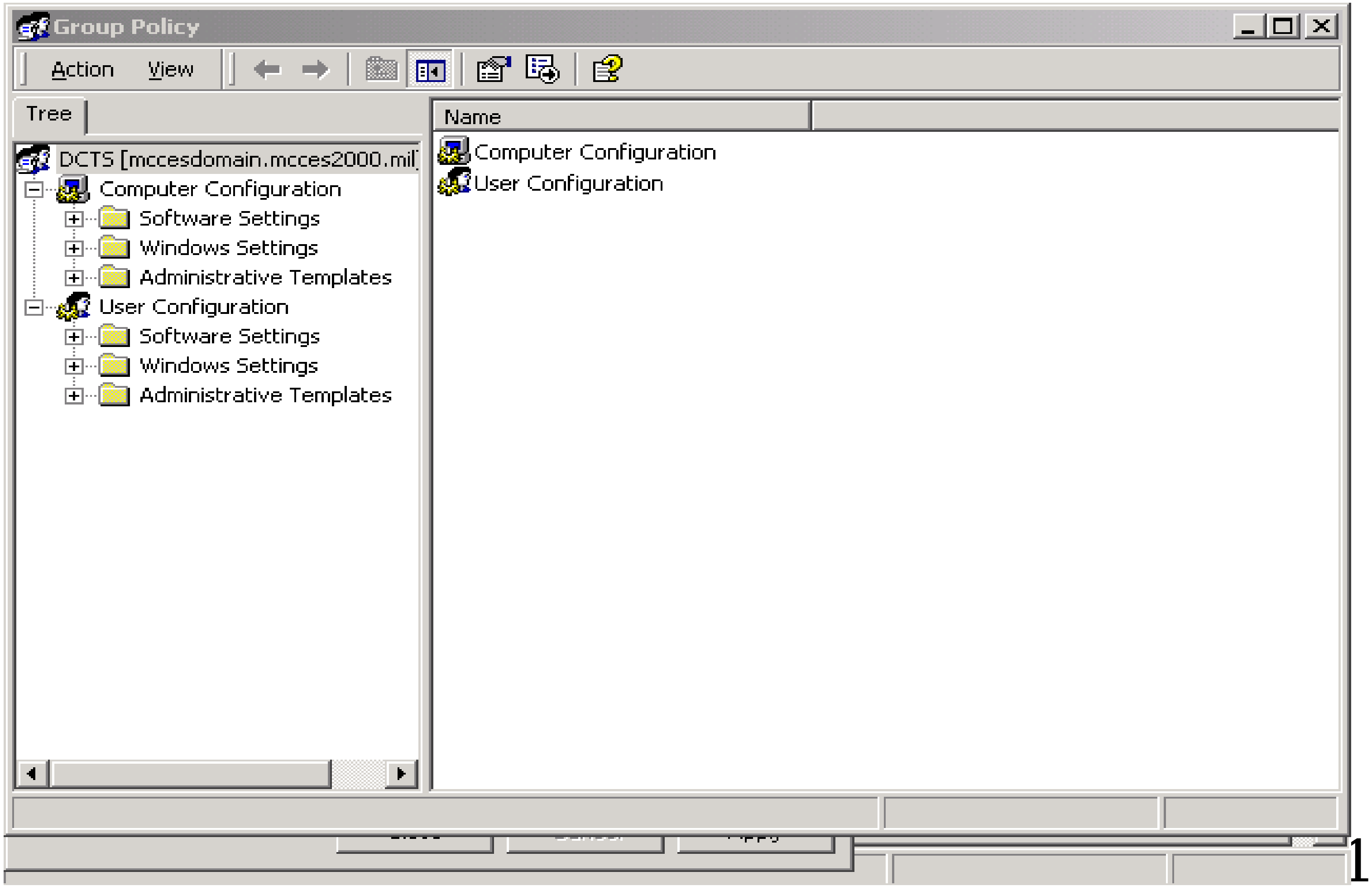
Group Policy Object Links	No Override	Disabled
Default Domain Controllers Policy		
New Group Policy Object		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: mccesdomain.mcces2000.mil

□ Block Policy inheritance

Managing Group Policy

- To edit an existing GPO assigned click EDIT



DCTS [mccesdomain.mcces2000.mil]
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

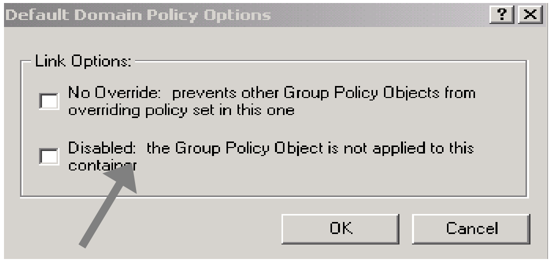
Computer Configuration
User Configuration

Permissions Requirements

- To edit a GPO
  - Users must have both Read and Write to the GPO
  - GPOs are not opened read-only
  - Must be an administrator, creator owner or a user delegated with the access to the GPO

Changes and Disabled Option

- Changes occur immediately
- Unlink a GPO from a domain, OU or site so it does not apply
- Located on the OPTIONS screen
- Turns off GPO to remove it from operation, but still associated with container specified
- Use when changing settings so as not to affect users policy
- Once editing is complete, clear the disabled checkbox



Default Domain Policy Options

Link Options:

□ No Override: prevents other Group Policy Objects from overriding policy set in this one

□ Disabled: the Group Policy Object is not applied to this container

Group Policy -- How it Affects Users

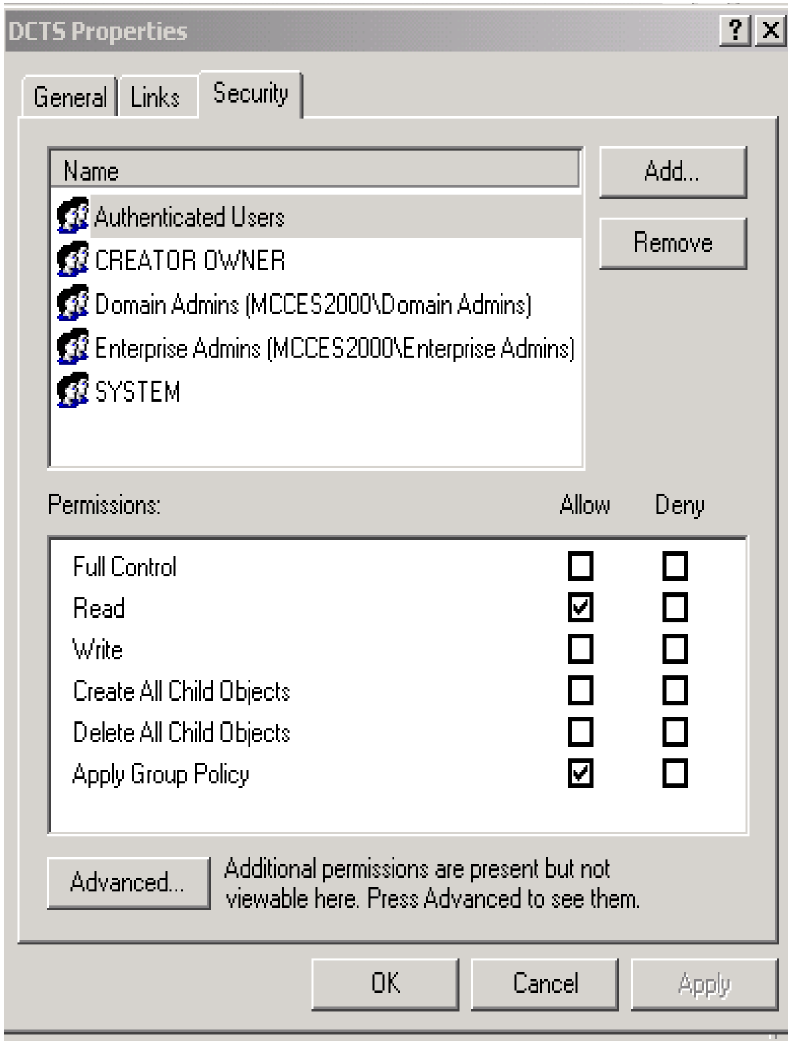
- All parts of the Group Policy Object settings modified, except Folder Redirection and Software Installation, are applied to all the security groups listed in the GPO permissions
- Some security groups are listed by default
- Selective parts can not be applied to users
  - If one option is to stop users from running Regedit, but displays the run command in the start menu, both options will be applied to the user
- Entire group policy settings are applied

GPO Permissions

- Default groups added to object
- Groups configured with a set of permissions
- Domain Admins, Enterprise Admins, System
  - Read, Write, Create All Child Objects, Delete All Child Objects, Edit of the GPO
- Authenticated Users
  - Read, Apply Group Policy (AGP)
- Creator Owner
  - Special Object and Attribute permissions assigned to child objects and properties within the GPO, Edit of the GPO

Modify GPO Permissions

- Select properties for site, domain, OU with GPO
- Select GPO, click properties and click Security tab
- Basic permission of Full Control, Read, Write, Create All Child Objects, Delete All Child Objects, and Apply Group Policy
- Advanced permissions



DCTS Properties

Name

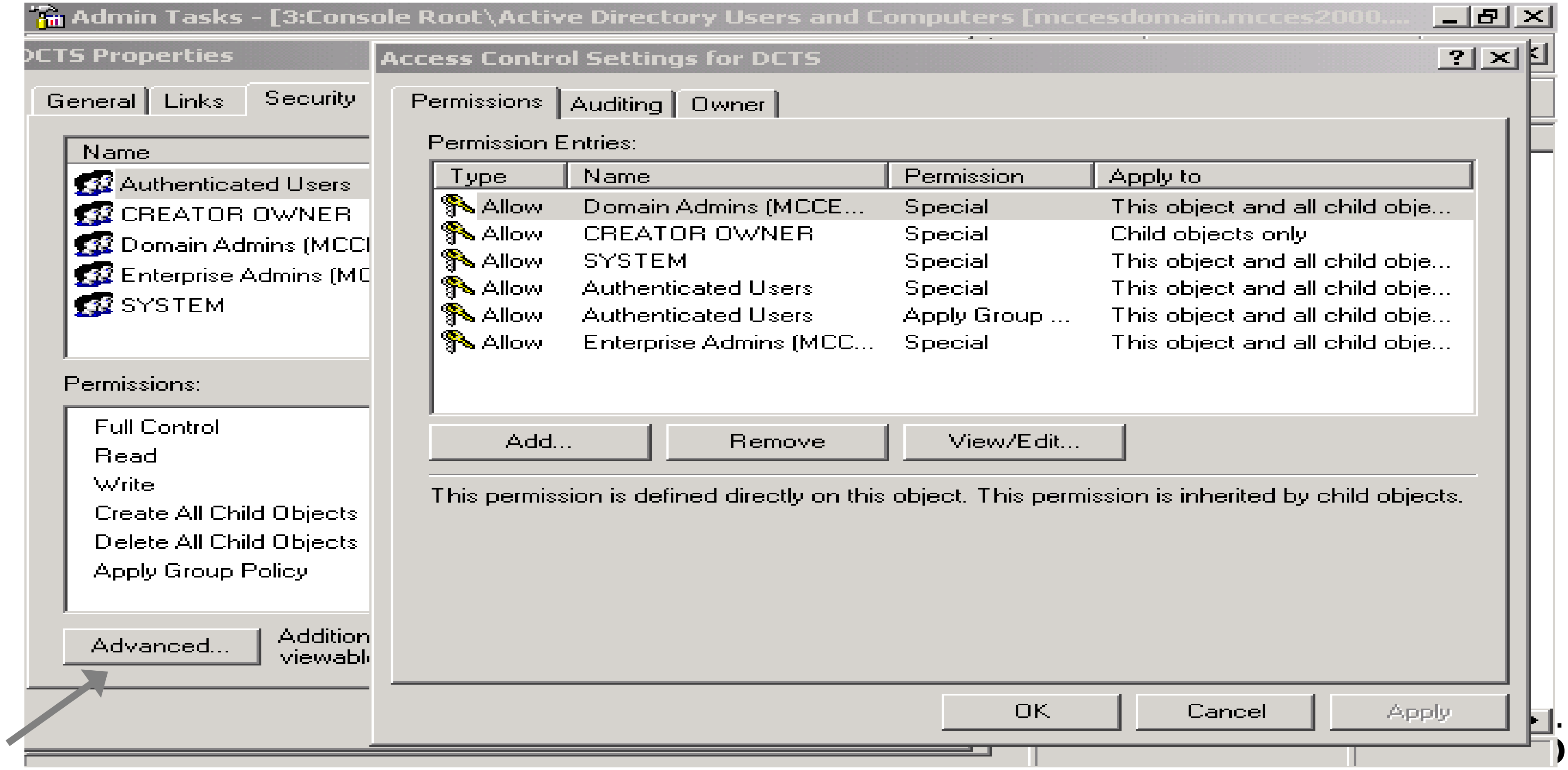
Authenticated Users
CREATOR OWNER
Domain Admins (MCCES2000\Domain Admins)
Enterprise Admins (MCCES2000\Enterprise Admins)
SYSTEM

Permissions:	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Apply Group Policy	☑	□

Additional permissions are present but not viewable here. Press Advanced to see them.

Advanced GPO Permissions

- Access Control Settings allow assigning Special Permissions thereby not using default roles


Admin Tasks - [3:Console Root\Active Directory Users and Computers [mccesdomain.mcces2000....
DCTS Properties
General
Links
Security
Access Control Settings for DCTS
Permissions
Auditing
Owner
Add...
Remove
View/Edit...
OK
Cancel
Apply
Advanced...
Addition
viewabl

Name

- Authenticated Users
- CREATOR OWNER
- Domain Admins (MCCI
- Enterprise Admins (MC
- SYSTEM

Permissions:

- Full Control
- Read
- Write
- Create All Child Objects
- Delete All Child Objects
- Apply Group Policy

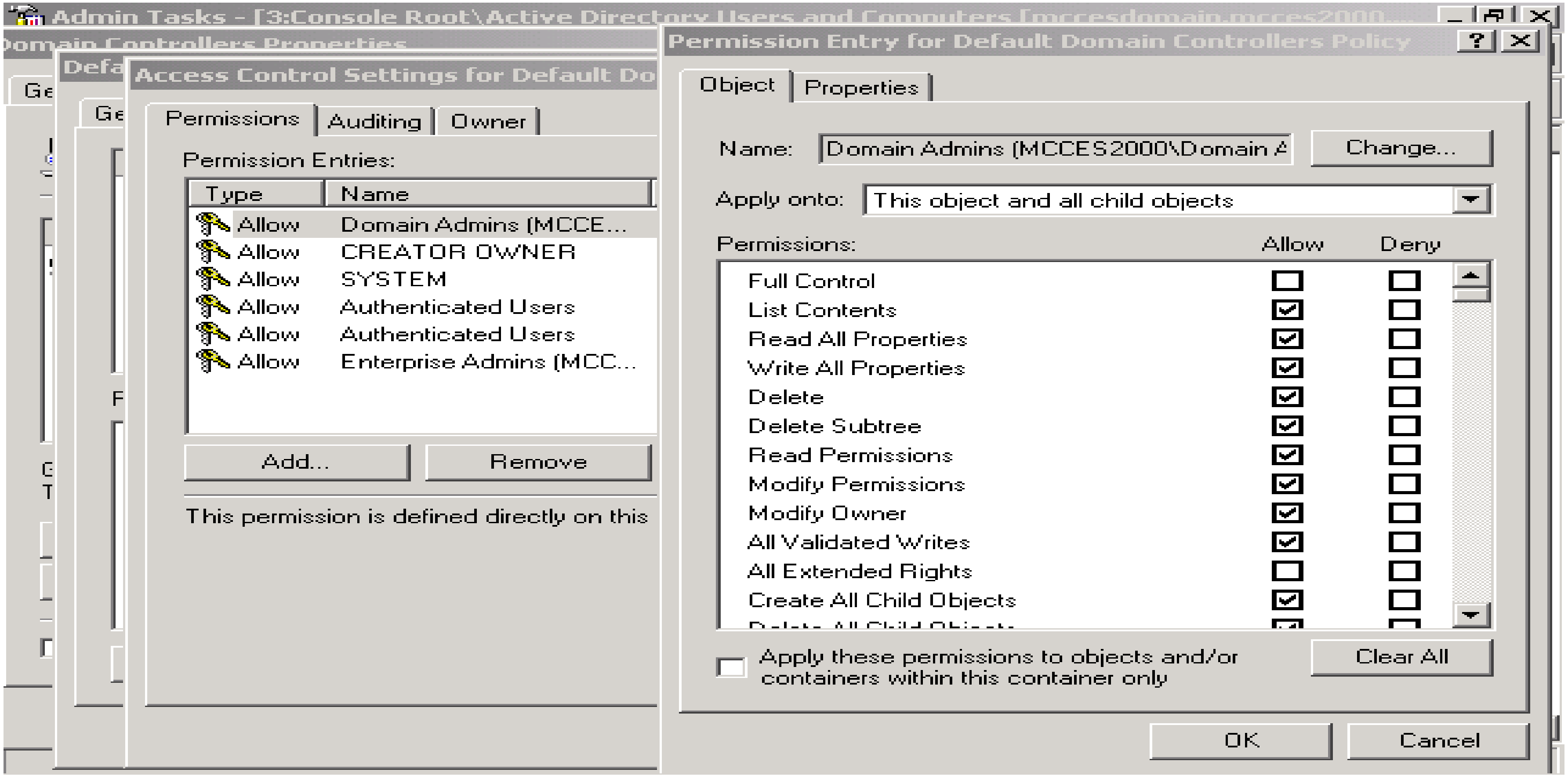
Permission Entries:

Type	Name	Permission	Apply to
Allow	Domain Admins (MCCE...	Special	This object and all child obje...
Allow	CREATOR OWNER	Special	Child objects only
Allow	SYSTEM	Special	This object and all child obje...
Allow	Authenticated Users	Special	This object and all child obje...
Allow	Authenticated Users	Apply Group ...	This object and all child obje...
Allow	Enterprise Admins (MCC...	Special	This object and all child obje...

This permission is defined directly on this object. This permission is inherited by child objects.

Changing “Special” Permissions

- Change advanced permissions: Add/Remove user/group or Edit/View exist permission



Admin Tasks - [3:Console Root\Active Directory Users and Computers [mccesdomain.mcces2000...
Domain Controllers Properties
Access Control Settings for Default Do
Permissions
Auditing
Owner
Add...
Remove
Permission Entry for Default Domain Controllers Policy
Object
Properties
Change...
Clear All
OK
Cancel

Permission Entries:

Type	Name
Allow	Domain Admins (MCCE...
Allow	CREATOR OWNER
Allow	SYSTEM
Allow	Authenticated Users
Allow	Authenticated Users
Allow	Enterprise Admins (MCC...

This permission is defined directly on this

Name: Domain Admins (MCCES2000\Domain A

Apply onto: This object and all child objects

Permissions:	Allow	Deny
Full Control	□	□
List Contents	☑	□
Read All Properties	☑	□
Write All Properties	☑	□
Delete	☑	□
Delete Subtree	☑	□
Read Permissions	☑	□
Modify Permissions	☑	□
Modify Owner	☑	□
All Validated Writes	☑	□
All Extended Rights	□	□
Create All Child Objects	☑	□
Delete All Child Objects	☑	□

□ Apply these permissions to objects and/or containers within this container only

Deny

- Policy settings do not apply to group members that have been denied Apply Group Policy permission (Deny)
- Administrators are part of the Authenticated Users group
- If don't want policy to apply to administrators, deny or remove Authenticated Users group from the default settings

Policy Inheritance

- GPs are passed from parent to child containers
- If assigned GP to a high-level parent container, that GP applies to all containers beneath the parent container including the user and computer objects in each container
- For instance, Group Policy set on the Domain level will flow down to the OU level

Policy Inheritance Concepts

- If the child container has been explicitly defined a GPO it overrides the parent policy
- If a parent OU has policy settings not configured, they are not inherited
- Disabled settings are inherited as disabled
- If a policy is configured for the parent OU and a policy is configured for a child OU and they are compatible (no conflicts), child inherits the parent policy and child is also applied

Policy Inheritance Exceptions

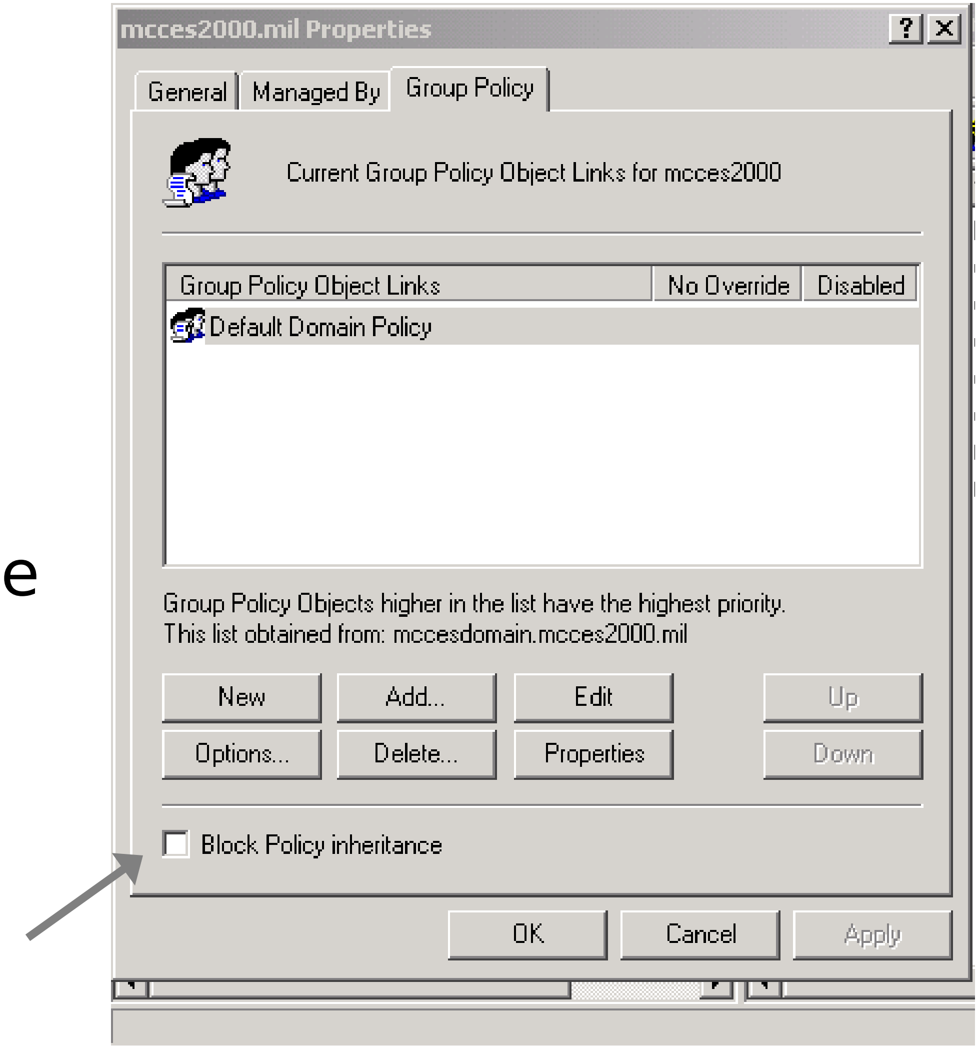
- If incompatible or the policies conflict, the child settings only apply to the child container/object.

Blocking

- Administrator's can configure inheritance
- Inheritance blocked for all policies from the levels above
- Performed at the domain or OU levels, not at the site level since top of hierarchy
- If multiple policies exist on the domain, NONE of the policies will filter to the OU that you have specified to block inheritance

How to Block Inheritance

- Block inheritance on child objects
  - Select the domain or OU properties
  - Select the Group Policy tab
  - Place a check in the box that says “Block Policy inheritance.”



mcces2000.mil Properties

General | Managed By | Group Policy

Current Group Policy Object Links for mcces2000

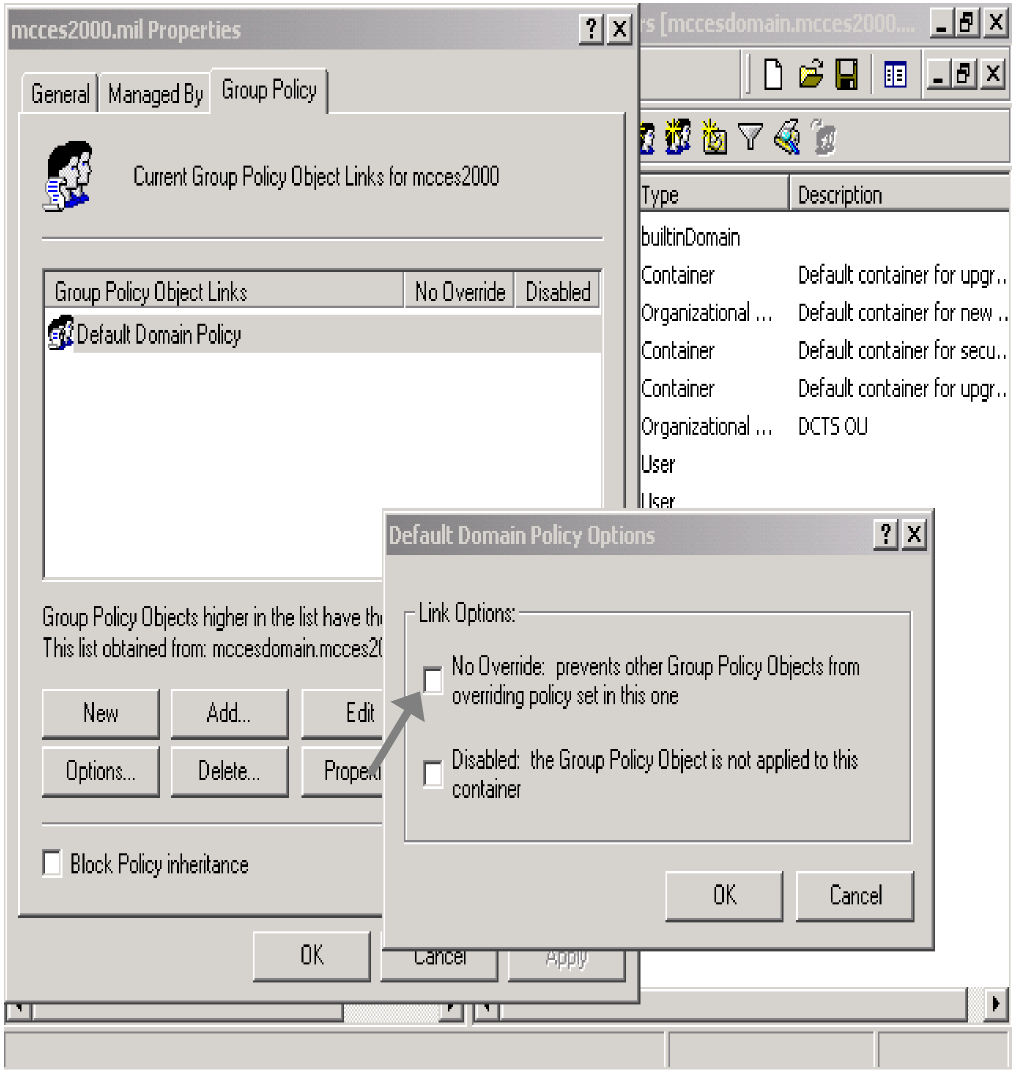
Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have the highest priority.
This list obtained from: mccesdomain.mcces2000.mil

□ Block Policy inheritance

No Override Option

- Forces child policy containers to inherit parent's policy even if those policies conflict with child properties; even with Block Inheritance checked
- Located on properties of GPO on the parent container by clicking the OPTIONS



mcces2000.mil Properties

General | Managed By | Group Policy

Current Group Policy Object Links for mcces2000

Group Policy Object Links	No Override	Disabled
Default Domain Policy		

Group Policy Objects higher in the list have th
This list obtained from: mccesdomain.mcces20

☐ Block Policy inheritance

s [mccesdomain.mcces2000....

Type	Description
builtinDomain	
Container	Default container for upgr..
Organizational ...	Default container for new ..
Container	Default container for secu..
Container	Default container for upgr..
Organizational ...	DCTS OU
User	
User	

Default Domain Policy Options

Link Options:

☐ No Override: prevents other Group Policy Objects from overriding policy set in this one

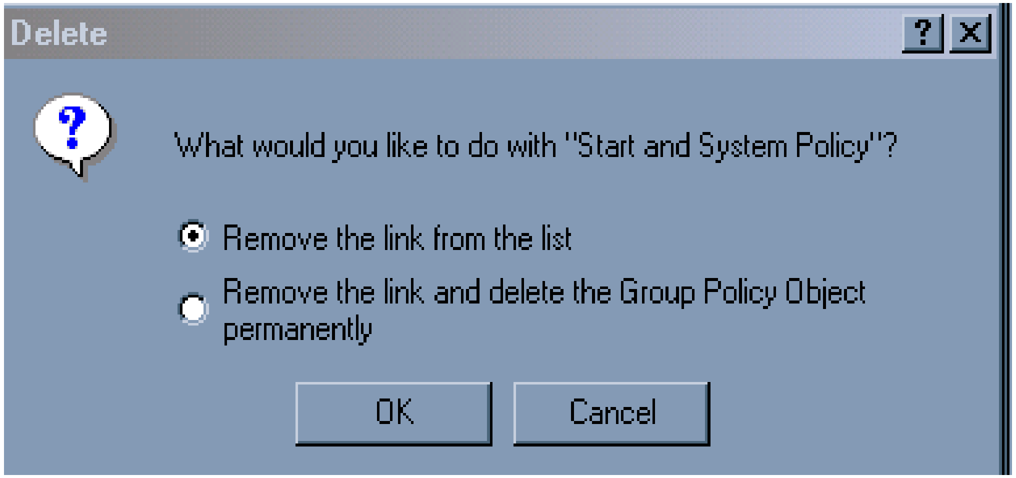
☐ Disabled: the Group Policy Object is not applied to this container

Deleting Policy

- DEFAULT DOMAIN POLICY GPO can NOT be deleted by an administrator
- Default Domain Policy contains required settings for the domain
- Can’t delete, but can disable the Computer and User configuration settings check boxes in the properties
- Can block inheritance if no override is not configured on the parent container

Administratively Created Policies

- Created policy that needs to be removed from site, domain or OU
- Need to delete a policy no longer required



What would you like to do with "Start and System Policy"?

● Remove the link from the list

○ Remove the link and delete the Group Policy Object permanently

- Procedure
  - Select policy
  - Select DELETE
  - Remove the link from list
  - Remove the link and delete GPO permanently

DFS

Managing the Distributed File System

- How the Distributed File System works
- How to create a Distributed File System root server
- How to add nodes and replicas to a Distributed File System root
- How to manage the Distributed File System

How DFS Works

- Without DFS, users must access shared resources in a *server-centric* fashion.
- DFS is designed to hide the server-centric view of network resources.
- users have to remember only two things:
  - the names of the DFS server
  - the DFS *root.*
  - You can name the DFS root anything you like.
  - DFS enables you to create a single virtual network resource that brings together all of the shared folders on all of your servers.

Reasons for using DFS

- You expect to add file servers or modify file locations.
- Users who access targets are distributed across a site or sites.
- Most users require access to multiple targets.
- Server load balancing could be improved by redistributing targets.
- Users require uninterrupted access to targets.
- Your organization has Web sites for either internal or external use.

Building a tree

- DFS works by building a tree.
  - The start of the tree is the DFS root
- You build the rest of the tree by adding *links*
  - A link is a single shared folder located on another computer
  - You provide the name of the link which does not have to be the same name as the shared folder

Providing references

1. A user types a UNC (or browses to one) that is on the DFS server—for

example, **\\MSTPDCEX01\home\UserFiles**.

2. The DFS server receives the request and looks up the UNC in the DFS tree.

3. The DFS server retrieves the actual shared folder UNC from the DFS tree and returns that UNC to the user's computer.

4. The user's computer directly accesses the UNC provided by the DFS server.

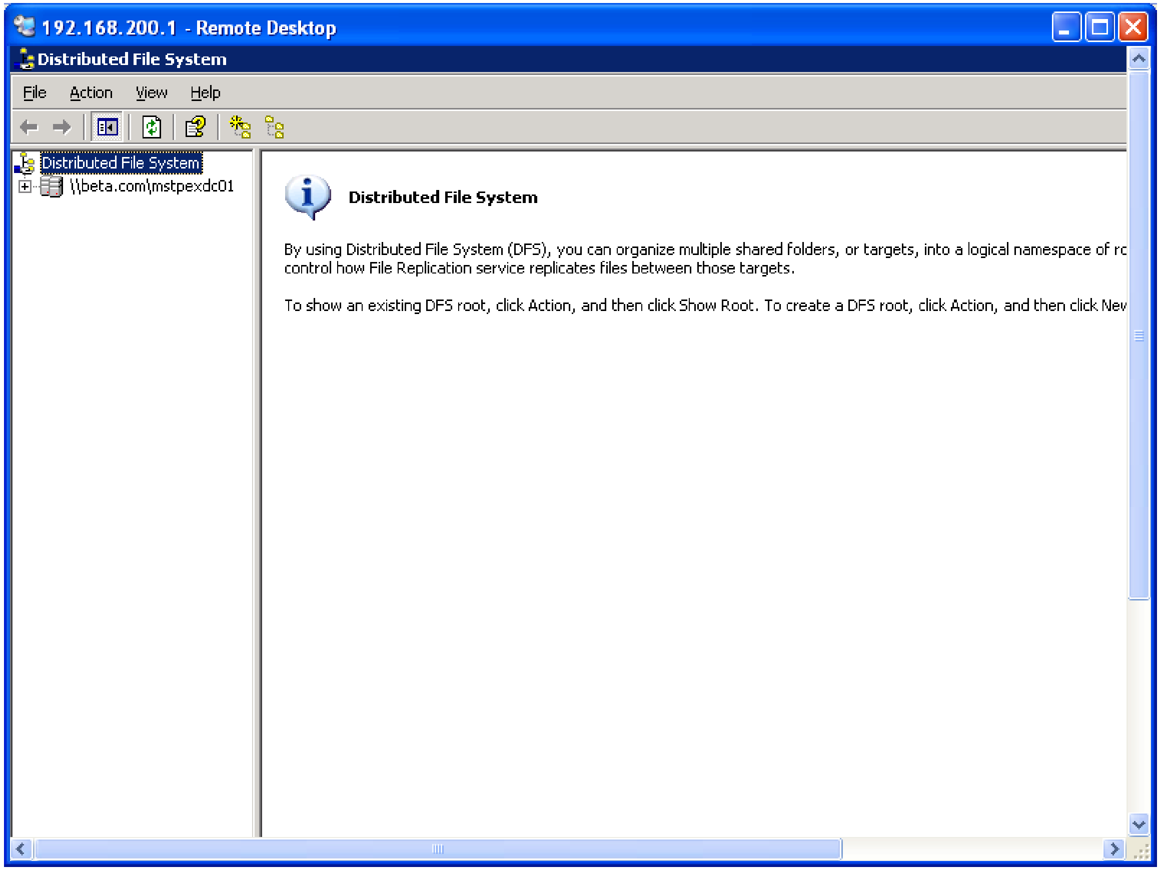
DFS does these steps transparently, so the user doesn't even realize it is happening.

Creating a DFS Root

You can create two types of DFS roots on a Windows Server 2003 computer:

- **Standalone.** A standalone DFS root runs on a Windows Server 2003 computer. The root exists only on that computer.
- **Domain-based.** A domain-based DFS root is stored in Active Directory. A member server may still act as the DFS server, but because the DFS tree itself is stored in Active Directory, it is protected by Active Directory’s own fault tolerance features.

Creating a DFS Root



Distributed File System

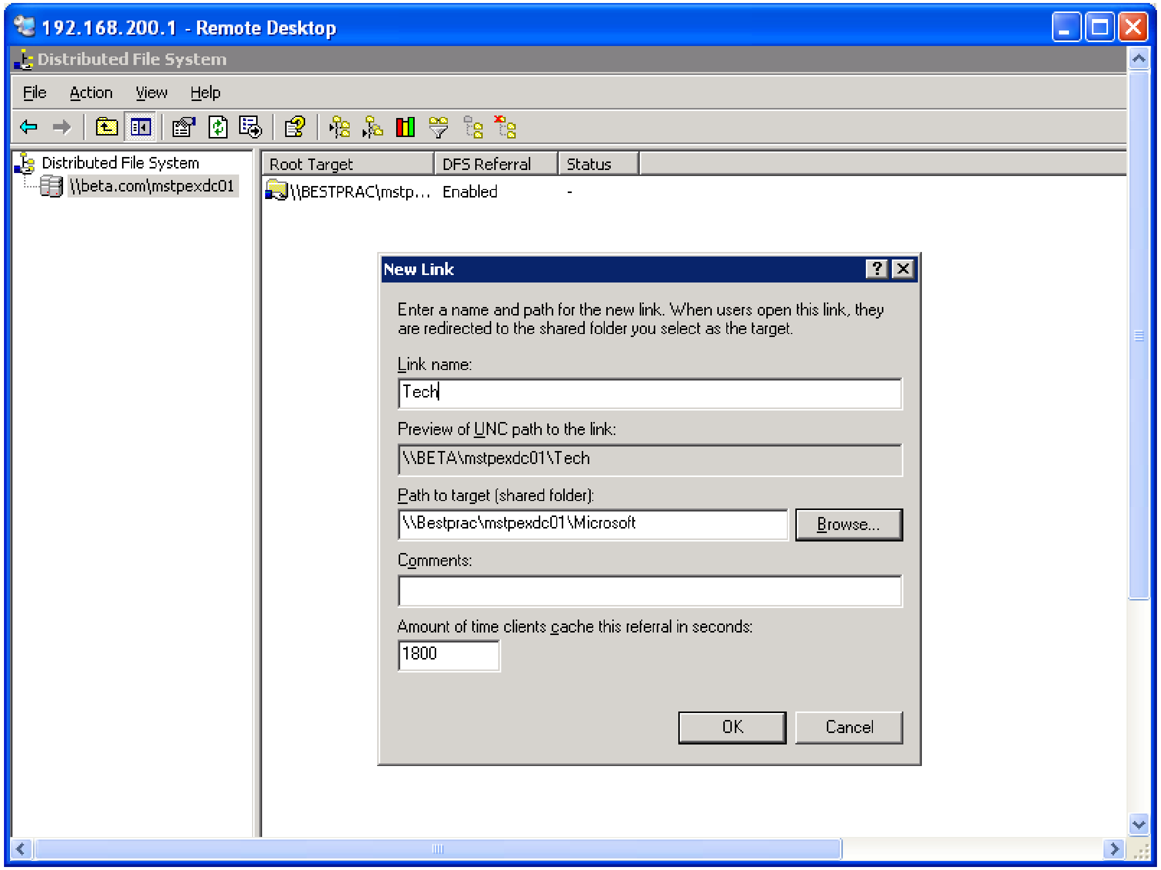
By using Distributed File System (DFS), you can organize multiple shared folders, or targets, into a logical namespace of rc
control how File Replication service replicates files between those targets.

To show an existing DFS root, click Action, and then click Show Root. To create a DFS root, click Action, and then click New

Adding DFS Links and Targets

- After creating your DFS root, you can begin adding links. DFS also enables you to add multiple shared folders for a single link, creating multiple targets. Multiple targets can be used to load- balance user requests across several identical shared folders.

Adding links



\\BESTPRAC\mstp... Enabled -

New Link

Enter a name and path for the new link. When users open this link, they are redirected to the shared folder you select as the target.

Link name: Tech

Preview of UNC path to the link: \\BETA\mstpexdc01\Tech

Path to target (shared folder): \\Bestprac\mstpexdc01\Microsoft

Comments:

Amount of time clients cache this referral in seconds: 1800

Adding target

- Once you’ve created a link, you can add multiple targets to it.
- Using multiple targets is a great way to help spread the burden associated with popular files on your network.

Never

Do not configure a link with multiple targets if users will be modifying the files in the shared folders. DFS does not automatically copy the changes made in one shared folder to the others, and so the targets will no longer contain identical content.

Managing DFS

Use the DFS console to manage DFS roots on the server

- To delete a DFS link target
- To filter the links that are displayed
- To temporarily prevent users from receiving referrals to a specific target

REVIEW

You learned how the Distributed File System (DFS) can be used to create a representation of your network's files and folders that is not server-centric. You learned how to create a DFS root, how to add DFS links to the root, and how to add multiple targets to DFS links. You also learned how multiple targets are used by DFS to load-balance access to shared files and folders. Finally, you learned how to perform day-to-day DFS administrative tasks using the DFS console.

QUIZ YOURSELF

MSTP

1. What happens when a DFS server receives a client request for a particular UNC?
2. How can you configure DFS to load-balance access to shared folders across multiple identical copies of the folder?
3. How can you make the DFS tree more fault tolerant, so that the failure of the DFS server will not necessarily result in the loss of the DFS tree data?
4. How does DFS enable clients to access shared folders on non-Windows servers?
5. What should you do in DFS if you need to move a shared folder to a different server?

Managing Disks, Files, and File Systems

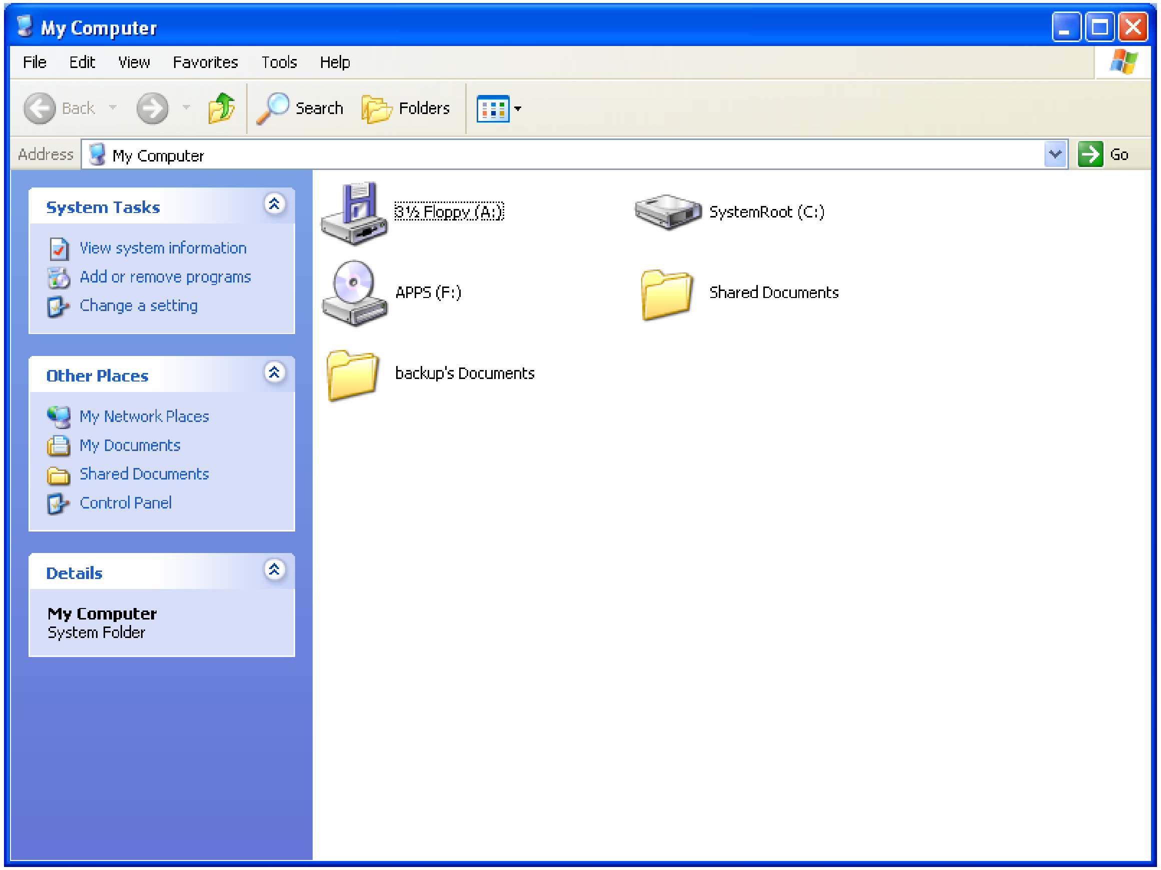
- How to configure disk drives
- How to use software fault tolerance
- How to select a file system and format disks
- How to optimize disk performance

Disks, Partitions, and Drives

- All new disks are referred to as *basic disks:*
  - cannot be used for special features like fault tolerance
- *logical drives*
  - they are assigned drive letters by the operating system
  - Drive letters A and B are reserved for the first two floppy disk drives
  - first hard drive partition is usually lettered C, the next one D

Drive assignments in a computer

MSTP



Address: My Computer

My Computer
System Folder

3½ Floppy (A:)

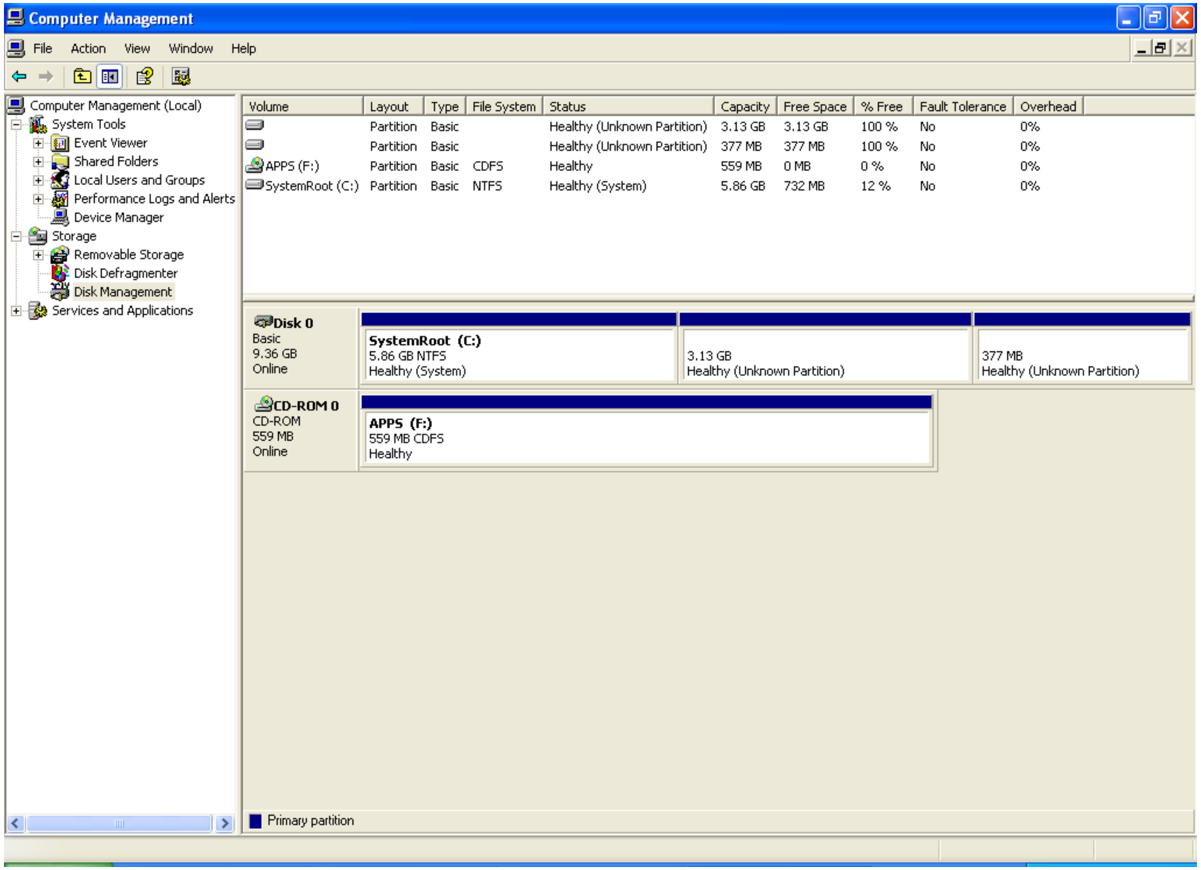
SystemRoot (C:)

APPS (F:)

Shared Documents

backup's Documents

Disk Management



Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free	Fault Tolerance	Overhead
	Partition	Basic		Healthy (Unknown Partition)	3.13 GB	3.13 GB	100 %	No	0%
	Partition	Basic		Healthy (Unknown Partition)	377 MB	377 MB	100 %	No	0%
APPS (F:)	Partition	Basic	CDFS	Healthy	559 MB	0 MB	0 %	No	0%
SystemRoot (C:)	Partition	Basic	NTFS	Healthy (System)	5.86 GB	732 MB	12 %	No	0%

Disk 0 Basic 9.36 GB Online	**SystemRoot (C:)** 5.86 GB NTFS Healthy (System)	3.13 GB Healthy (Unknown Partition)	377 MB Healthy (Unknown Partition)
CD-ROM 0 CD-ROM 559 MB Online	**APPS (F:)** 559 MB CDFS Healthy		

■ Primary partition

Disk Management

You can use Disk Management to accomplish several important tasks:

- To create a new partition, right-click the empty area of a hard disk and select Create Partition from the pop-up menu.
- To change the drive letter assigned to a CD-ROM or partition, right-click it and select Drive Letters from the pop-up menu.
- To convert a basic disk to a *dynamic disk*, which supports more partitions as well as special features like fault tolerance, right-click the disk and select Convert to Dynamic Disk from the pop-up menu.
- To remove a partition, right-click it and select Delete from the pop-up menu.

Fault Tolerance

- Windows Server 2003 helps prevent such losses by providing two levels of software-based fault tolerance: mirroring and RAID 5.

Mirroring

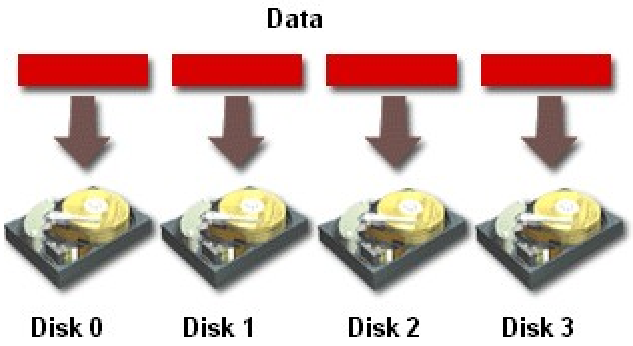
- Mirroring allows two identically sized partitions, located on separate disks, to automatically duplicate one another.
- Both partitions become a *mirror set,* which means they always contain the same content and appear to the operating system as if they were a single partition.
  - Mirror sets use only one drive letter
  - Disk Management gives you the tools necessary to work with mirror sets:

RAID 5

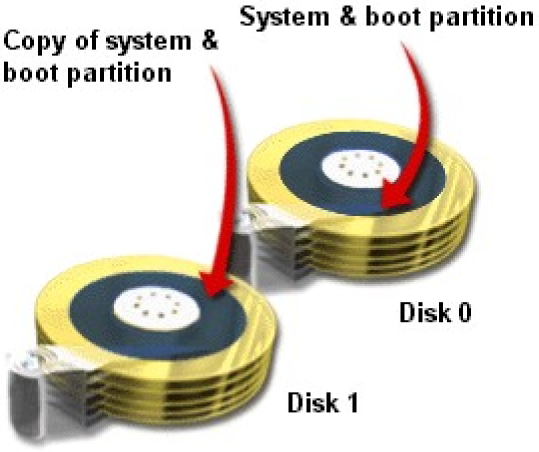
- **RAID is an acronym that stands for *Redundant Array of Inexpensive Devices.***
  - can help improve fault tolerance
  - **speed up the process of reading**

- **RAID 5 arrays consist of at least three partitions of equal size:**
  - RAID 5 volumes can be created only by using identically sized empty areas of dynamic disks.
  - The operating system saves data to all of the array partitions at once dividing saved information between them
  - The operating system calculates *checksum data.*
  - If one disk in a RAID 5 array fails, the checksum data from the remaining drives is used to recreate the data that was stored on the failed disk.
  - If two or more disks in the array fail, then all of the data on the array is lost.

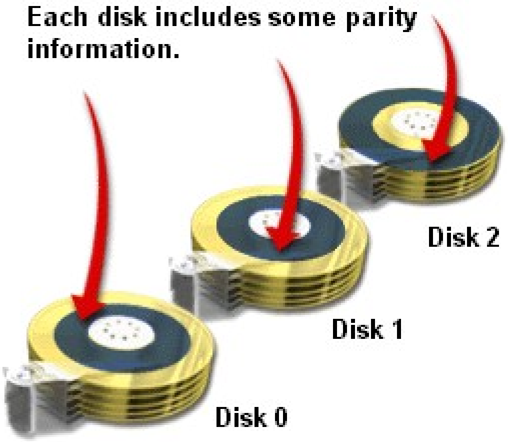
Raid



Raid Level 1 - Mirror



Raid Level 5 – Stripe Set with Parity



REVIEW

You learned about Windows Server 2003’s organization of the disks in your computer, including basic disks and dynamic disks. You learned how to create partitions on a disk, select a file system for the partition, format the partition, and assign a drive letter to the partition. You also learned about Windows Server 2003’s software fault tolerance features, including the ability to create mirror sets and RAID 5 arrays by using the Disk Management application. Finally, you learned some tips for optimizing the disks in your computer, such as striped sets.

QUIZ YOURSELF

1. What kinds of disk fault tolerance does Windows Server 2003 offer?

2. What three main file systems does Windows Server 2003 support?

3. What are the advantages of the NTFS file system?

4. How can you change the drive letter associated with a specific partition?

5. When a new drive is added to a computer, what type of disk does Windows Server 2003 configure it as?

Advanced File Management

- How to compress files on a hard disk
- How to encrypt and decrypt files on a hard disk
- How to manage disk space using quotas

File Compression

- Windows Server 2003 has the ability to compress files stored on any NTFS volume.
  - When compression is used, files take up less space on disk.
  - The operating system automatically decompresses files that are being accessed, so client computers don’t need to have any special compression software installed.
  - The operating system also recompresses files that are changed and then saved, ensuring that the file uses as little disk space as possible.

Performance impact of compression

- Windows Server 2003 requires extra time when a user accesses a compressed file
- The operating system has to decompress (and recompress, if the file is changed and then saved) the file
  - The performance impact decompress a single file is very small
  - large number of compressed files, the additional work performed by the server becomes quite noticeable and can make the server seem unusually slow to respond.
    - Compression is most commonly used on files that are not used very often.

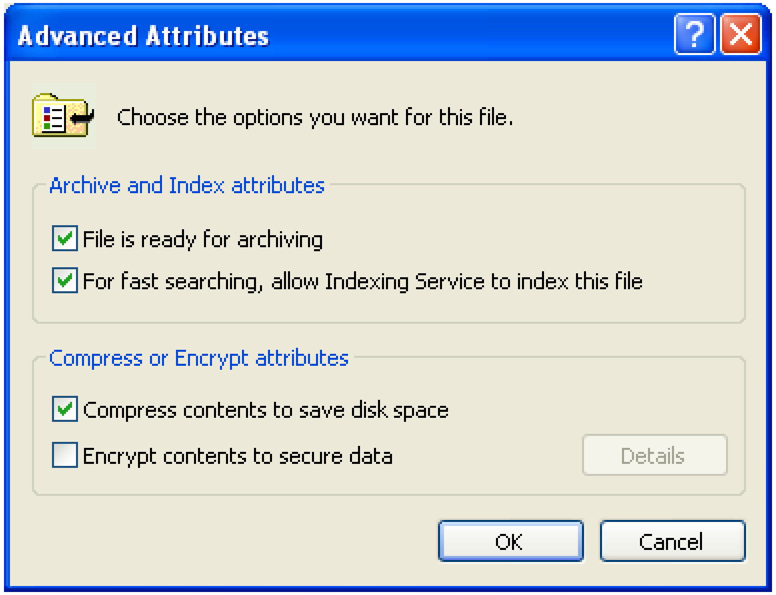
Compression

Other files that might be eligible for compression include:

- Last year's accounting files, which aren't regularly needed but still must be available at a moment's notice.
- Old customer files, which might be needed in an emergency but are otherwise seldom used.
- Other archived data, which is accessed often enough to keep it on the server, but usually less than once or twice a week.

How to use compression

By default, Windows Server 2003 displays the names of compressed files and folders in b



Advanced Attributes

Choose the options you want for this file.

Archive and Index attributes

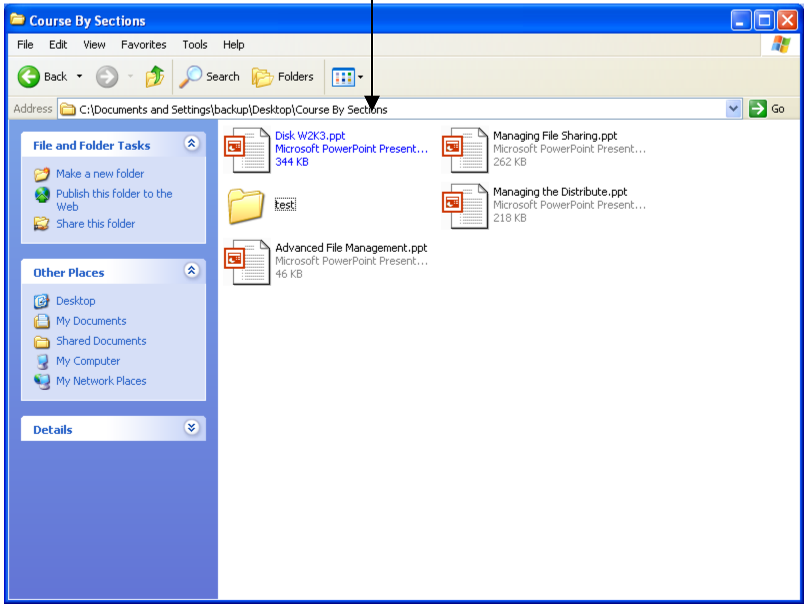
☑ File is ready for archiving

☑ For fast searching, allow Indexing Service to index this file

Compress or Encrypt attributes

☑ Compress contents to save disk space

☐ Encrypt contents to secure data



Course By Sections

Address C:\Documents and Settings\backup\Desktop\Course By Sections

Disk W2K3.ppt
Microsoft PowerPoint Present...
344 KB

Managing File Sharing.ppt
Microsoft PowerPoint Present...
262 KB

test

Managing the Distribute.ppt
Microsoft PowerPoint Present...
218 KB

Advanced File Management.ppt
Microsoft PowerPoint Present...
46 KB

Rules for compressed files and folders

- Compressed files remain compressed if they are moved to a new location on the same volume. Compressed files moved to a different volume take on the compression attribute of the folder they are placed into.
- Compressed files that are copied always take on the compression attribute of the folder they are copied to. The original file remains compressed.
- Compressed folders follow the same rules as compressed files.

- **Only the NTFS file system supports file compression. If you want to compress files on any other file system, use the Compressed Folders feature or a third-party archiving application like WinZIP.**

File Encryption

- Windows Server 2003 provides the Encrypting File System (EFS).
  - EFS uses digital encryption keys to encode files so that only the owner, and users the owner designates, can access the files.

Performance of encryption

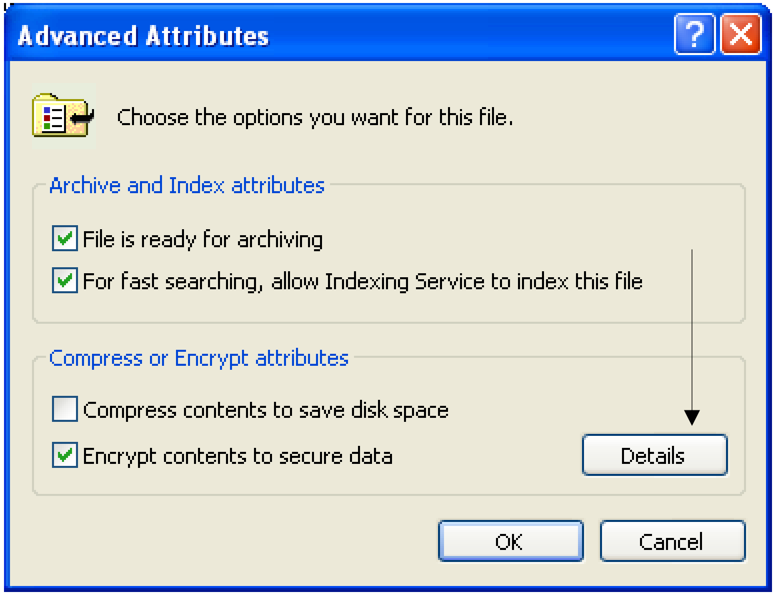
- Similar to the extra time required for file compression,
  - Windows Server 2003 requires extra time to encrypt and decrypt files.
  - If a large number of users attempt to access a large number of encrypted files, the server may seem slow to respond.
    - Generally, only especially sensitive files are encrypted, so the negative performance impact of encryption is minimal.
- minimize the performance overhead of encryption is to encrypt only individual files.

Encryption

- When you encrypt a folder, Windows Server 2003 automatically encrypts the files within that folder, as well as any new files added to the folder.
  - The folder itself isn't encrypted; it is simply marked so that future files placed within it will be automatically encrypted.

How to use encryption

- You can encrypt files and folders using the same procedure you use to compress them.
- **You cannot apply both compression and encryption to the same files or folders. If you select one option, the other is automatically cleared. You have to choose one or the other.**
- When you encrypt a file, Windows Server 2003 asks if you want to encrypt only the file, or if you want to encrypt the file and its parent folder.
- By default, only the user who encrypts a file can decrypt it.



Advanced Attributes

Choose the options you want for this file.

Archive and Index attributes

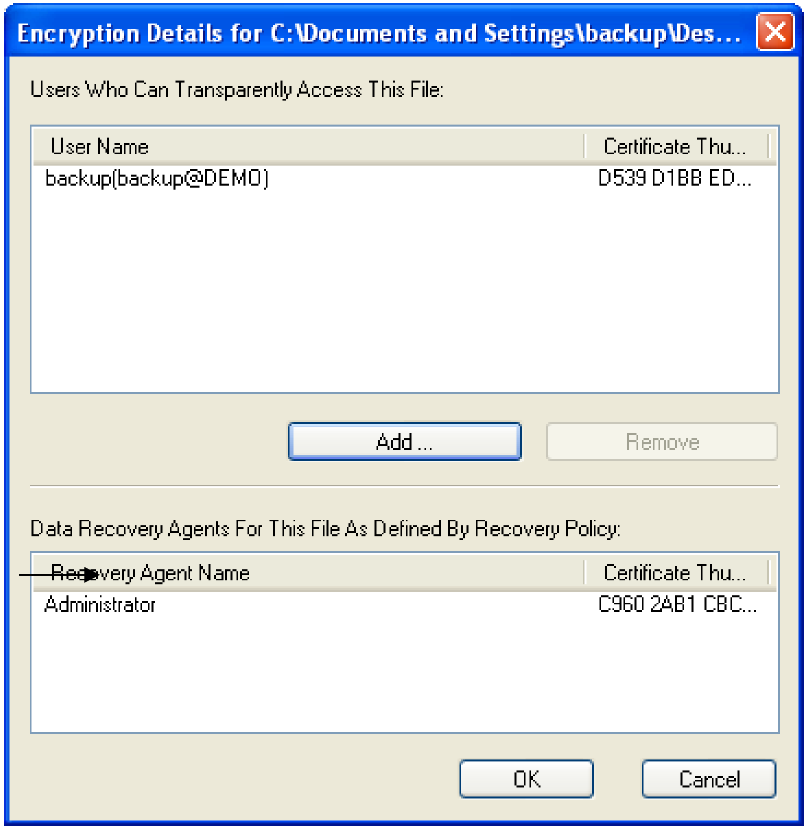
☑ File is ready for archiving

☑ For fast searching, allow Indexing Service to index this file

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data



Encryption Details for C:\Documents and Settings\backup\Des...

Users Who Can Transparently Access This File:

User Name	Certificate Thu...
backup(backup@DEMO)	D539 D1BB ED...

Data Recovery Agents For This File As Defined By Recovery Policy:

Recovery Agent Name	Certificate Thu...
Administrator	C960 2AB1 CBC...

Rules for encrypted files and folders

Encryption follows the same rules for moving and copying as file compression

- Encrypted items that are moved on the same volume retain their encryption;
- items moved to a different volume, or copied, take on the encryption attribute of their new folder.
- Remember that only the user who encrypts a file (or users they permit) can decrypt it.

Recovering encrypted files

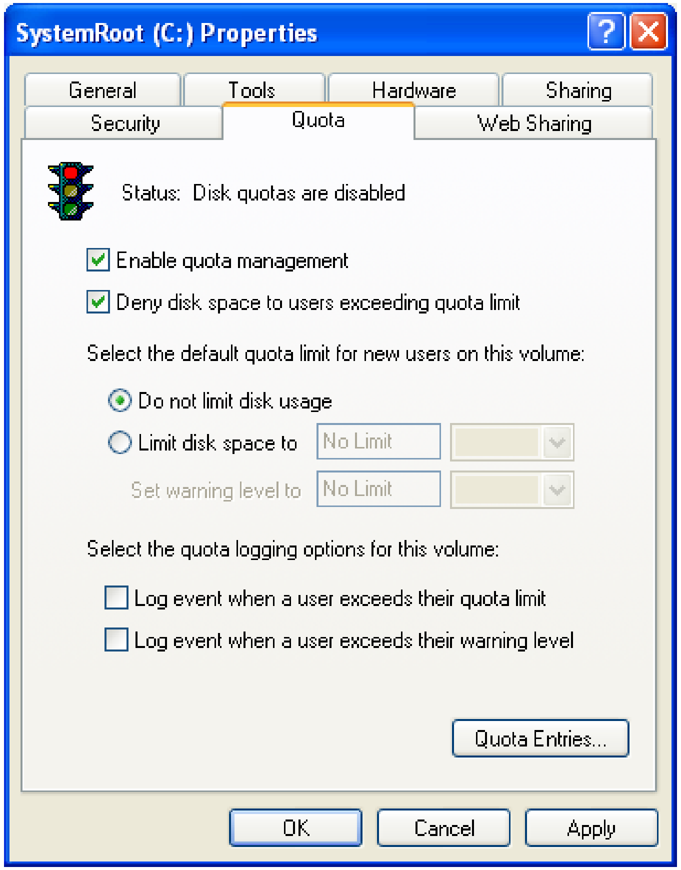
- Domain administrators define recovery agents using domain security policy.
  - “recovery agents”
    - The agents can decrypt any encrypted file.
  - To do so, they must back up the encrypted file,
    - restore it to a secure computer,
    - log on as a recovery agent, and decrypt the file

Disk Quotas

- One of the most common uses for Windows Server 2003 is as a file server:
  - a central repository where users can store their data files.
- Disk quotas were created to help manage how users utilize server disk space.
  - Quotas assign specific space limitations (called *thresholds*) to specific users.
    - The thresholds apply for an entire volume, and users who exceed the threshold can be cut off—preventing them from using any more disk space.

Using disk quotas

- **Deny disk space to users exceeding quota limit.** Check this check box to prevent users from using any more disk space once they exceed their quota threshold.
- **Limit disk space to.** This option enables you to specify the maximum amount of disk space each user can utilize on the volume.
- **Set warning level to.** This option warns users that they are approaching their quota limit when they reach the designated utilization level. This option should be set at a lower level than the "Limit disk space to" option.
- **Logging options.** The two logging options cause Windows .NET Server 2003 to create an Event Log entry whenever a user exceeds the warning limit you set or when they exceed their quota limit.



Status: Disk quotas are disabled

☑ Enable quota management

☑ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

● Do not limit disk usage

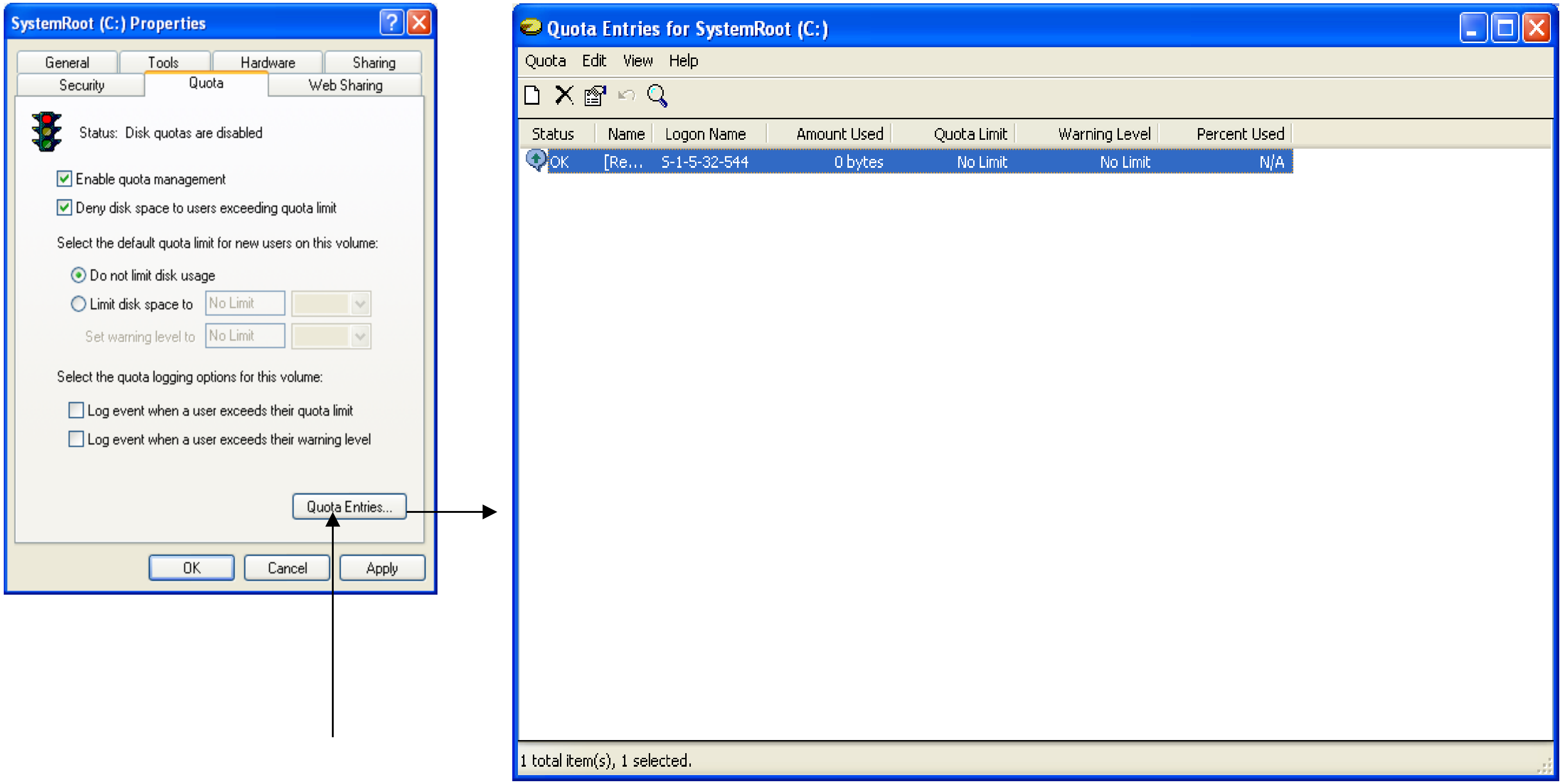
○ Limit disk space to No Limit

Set warning level to No Limit

Select the quota logging options for this volume:

□ Log event when a user exceeds their quota limit

□ Log event when a user exceeds their warning level



SystemRoot (C:) Properties

Status: Disk quotas are disabled

☑ Enable quota management

☑ Deny disk space to users exceeding quota limit

Select the default quota limit for new users on this volume:

● Do not limit disk usage

○ Limit disk space to No Limit

Set warning level to No Limit

Select the quota logging options for this volume:

□ Log event when a user exceeds their quota limit

□ Log event when a user exceeds their warning level

Quota Entries for SystemRoot (C:)

Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
OK	[Re...	S-1-5-32-544	0 bytes	No Limit	No Limit	N/A

1 total item(s), 1 selected.

To create a quota entry, click the Quota Entries button.

Disk quotas and compression

- What if your users compress some of their files?
  - Windows Server 2003 uses the *uncompressed* file size in quota calculations, regardless of how much disk space the file is actually using.

REVIEW

You learned how to use file compression to compress files so that they use less disk space than they normally would. You also learned how to use file encryption to protect sensitive files and how to recover encrypted data if necessary. You also learned how to use disk quotas to limit the amount of disk space users can fill up on your servers.

QUIZ YOURSELF

1. What happens if you move a compressed file to a different hard disk?

2. What happens if you mark a folder for encryption and then create a new Notepad file in that folder?

3. Can you encrypt and compress a file at the same time?

4. What types of restrictions can you apply using disk quotas?

5. How does file compression interact with disk quotas?

DISASTER RECOVERY

Performing Disaster Recovery Operations

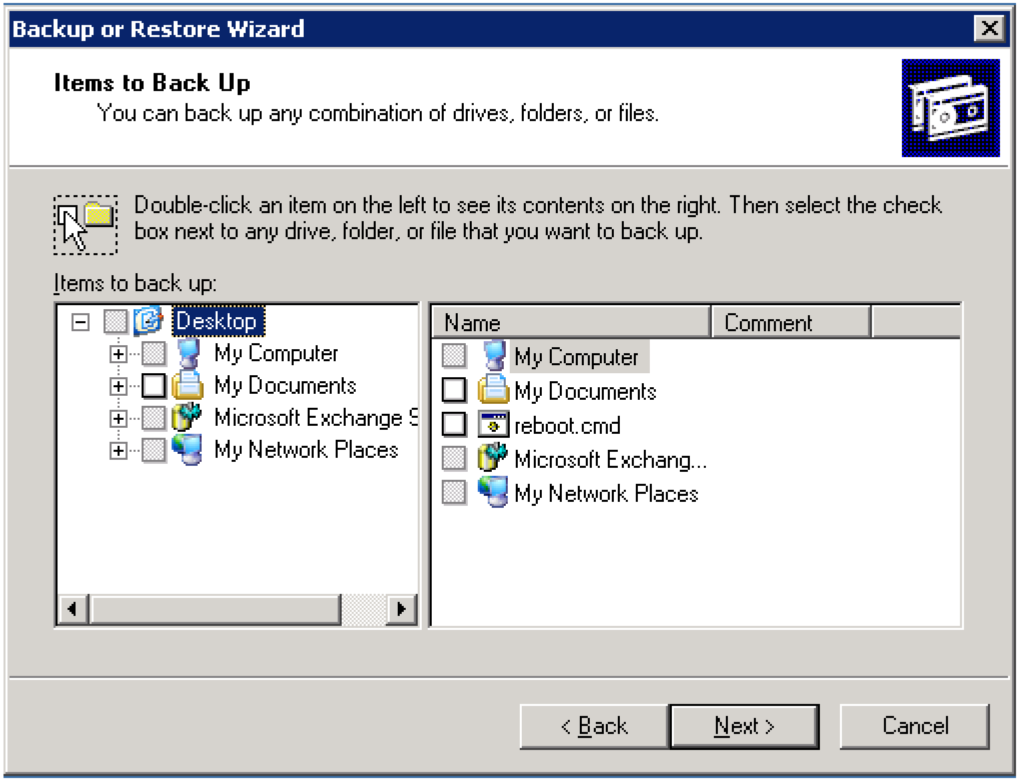
- How to back up and restore data
- How to install the Recovery console
- How to use Automatic System Recovery

Backup and Restore

- Windows Server 2003 includes a basic backup and restore application called Windows Backup.
  - back up the files on any computer on your network, and to back up the *system state* of the local computer to a backup file on disk or tape
- Back up the system state of computers across the network (the built-in application can back up only the local computer’s system state).
- Schedule backups that include several computers across the network (while you can do this with the built-in application, it’s cumbersome and timeconsuming).
- Manage a large set of backup media, such as tapes or optical disks.

Backing up data

- Windows Backup enables you to back up files and the local computer's system state.
- Windows Backup can back up data either to a disk-based file or to a backup tape.



Backup or Restore Wizard

Items to Back Up

You can back up any combination of drives, folders, or files.

Double-click an item on the left to see its contents on the right. Then select the check box next to any drive, folder, or file that you want to back up.

Items to back up:

Types of backups

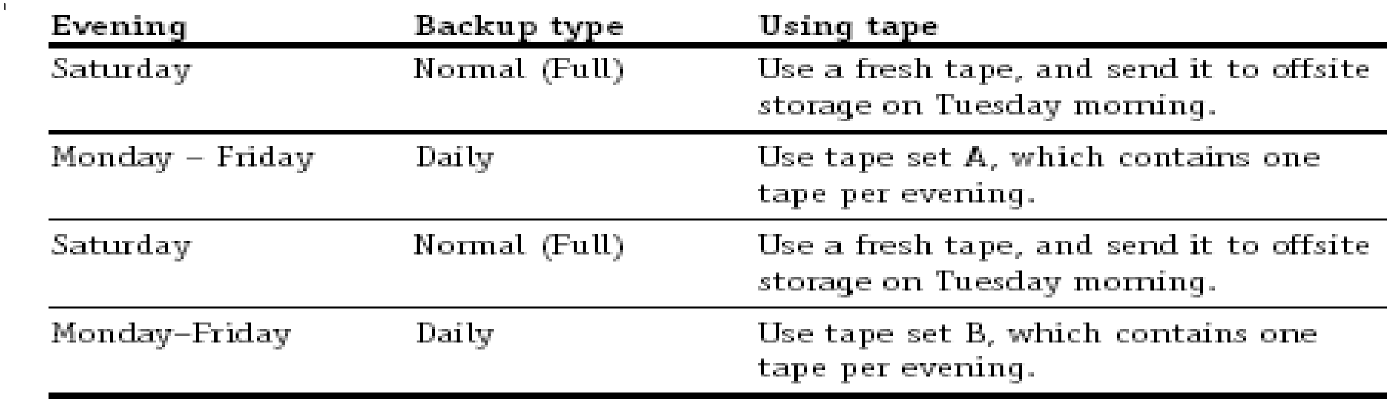
- **Normal backup.** Also referred to as a Full backup, a Normal backup backs up all the files you select. It clears the archive bit on each file.
- **Daily backup.** Backs up only the files whose “last changed” dates match the current date. The backup does not modify the archive bit on each file that it backs up. The Daily backup is intended to catch all the files that have changed that day.
- **Incremental backup.** Backs up all files whose archive bits are set, and it clears the archive bits. The Incremental backs up any files that have changed since the last Full or Incremental backup.

Cont.

- **Full backup.** When restoring, you need the most recent Full backup, and every Incremental backup performed since the Full backup, in order to restore all of the files on your server to their most recent condition.
- **Differential backup.** Backs up all the files whose archive bits are set, but it does not clear them. Subsequent Differential backups back up the same files, so Differentials grow progressively larger until a Full or Incremental backup is performed.

Managing backup tapes

- If you back up data to tape, you should establish a tape rotation schedule



Evening	Backup type	Using tape
Saturday	Normal (Full)	Use a fresh tape, and send it to offsite storage on Tuesday morning.
Monday – Friday	Daily	Use tape set A, which contains one tape per evening.
Saturday	Normal (Full)	Use a fresh tape, and send it to offsite storage on Tuesday morning.
Monday–Friday	Daily	Use tape set B, which contains one tape per evening.

Restoring data

- Windows Backup enables you to restore data that you backed up earlier.

The Recovery Console

- The Recovery console is a special command-line interface that you can use to help perform troubleshooting and recovery tasks on your server.

  To install the Recovery console, insert the Windows Server 2003 CD into the server.
- From the Start menu, select Run, and type **d:\i386\winnt32.exe /cmdcons**, replacing **d:\** with the letter of the CD-ROM drive on your server.
- The Recovery console appears as an additional operating system selection on the server’s startup menu.

Automatic System Recovery

- Windows Automatic System Recovery (ASR) is a last-resort process you can use to restore your server’s operating system to full functionality.
  - ASR does not restore your data files, and ASR does require that you perform a special ASR backup before ASR can be used.

ASR backup

- You use Windows Backup to perform an ASR backup. Open Windows Backup and, if you’re in Advanced mode, select ASR Wizard from the Tools menu.
- The ASR Backup Wizard automatically backs up the files required to perform an ASR restore. ASR *does not include your data files,* so make sure you perform a regular backup of those files once the ASR backup is complete.

ASR restore

- If your server fails and all attempts to restore it to operation also fail, you can resort to an ASR restore.

REVIEW

You learned about the importance of disaster recovery preparation, and you learned how to use Windows Server 2003’s built-in tools for backup and restore, system snapshots, and Automatic System Recovery (ASR). You also learned how to install and log on to the Recovery console.

The greatest disadvantage to RAID 5 arrays

- available disk space is sacrificed to store the checksum information.
- total disk space equals the space available on all but one of the disks in the array
  - For example, in an array with five 10GB disks, you have a total of 40GB of available space.

File Systems

- **FAT16.** The FAT16 file system is compatible with older operating systems like MS-DOS and Windows 95.
- **FAT32.** The FAT32 file system is more efficient than FAT16 and is compatible with Windows 98 and Windows Me (as well as later versions of Windows 95).
- **NTFS.** The NTFS file system is the best file system to use with Windows Server 2003.
  - You need to *format* the partition with the file system.
  - Formatting is a process that organizes the partition and allows the operating system to begin saving data to it

Disk Optimization

- ***Using disks carefully***
  - Carefully planning how the disks in your computer are used can help improve disk performance.
    - use one hard drive for the operating system files and another hard drive for user data files.
  - A better solution is to use one drive for the operating system files and make a RAID 5 array from the remaining three drives.

Stripe sets for better performance

- Windows Server 2003 supports a special type of volume called a *stripe set.*
  - stripe sets spread data across several identically sized disks
  - speeds up the process of reading data
  - stripe sets do not calculate checksum information
  - stripe sets do not provide fault tolerance
  - if one disk should fail, all of the data on the stripe set will be lost.

Disaster Recovery and Planning

- System State
- Time Frame for the inevitable
  - Backup time
  - Restore time
- Hard Drive Redundancy
- Server Protection
  - UPS

Disaster Recovery

Fix or replace broken hardware	Unknown
Install Windows 2000	90 minutes
Restore Full System from Tape	Depends on tape – 2-4 hours is reasonable
Reboot and review services	At least an hour
Restore Databases or Additional user	Depends on size

Disaster Recovery

Local Administrator Password	Frequently forgotten, will be restored. Domain admin password will not work
Disk configurations and signatures (in case of cluster)	Disk configuration will need to be rebuilt manually
A backup set	No tape? No restore!

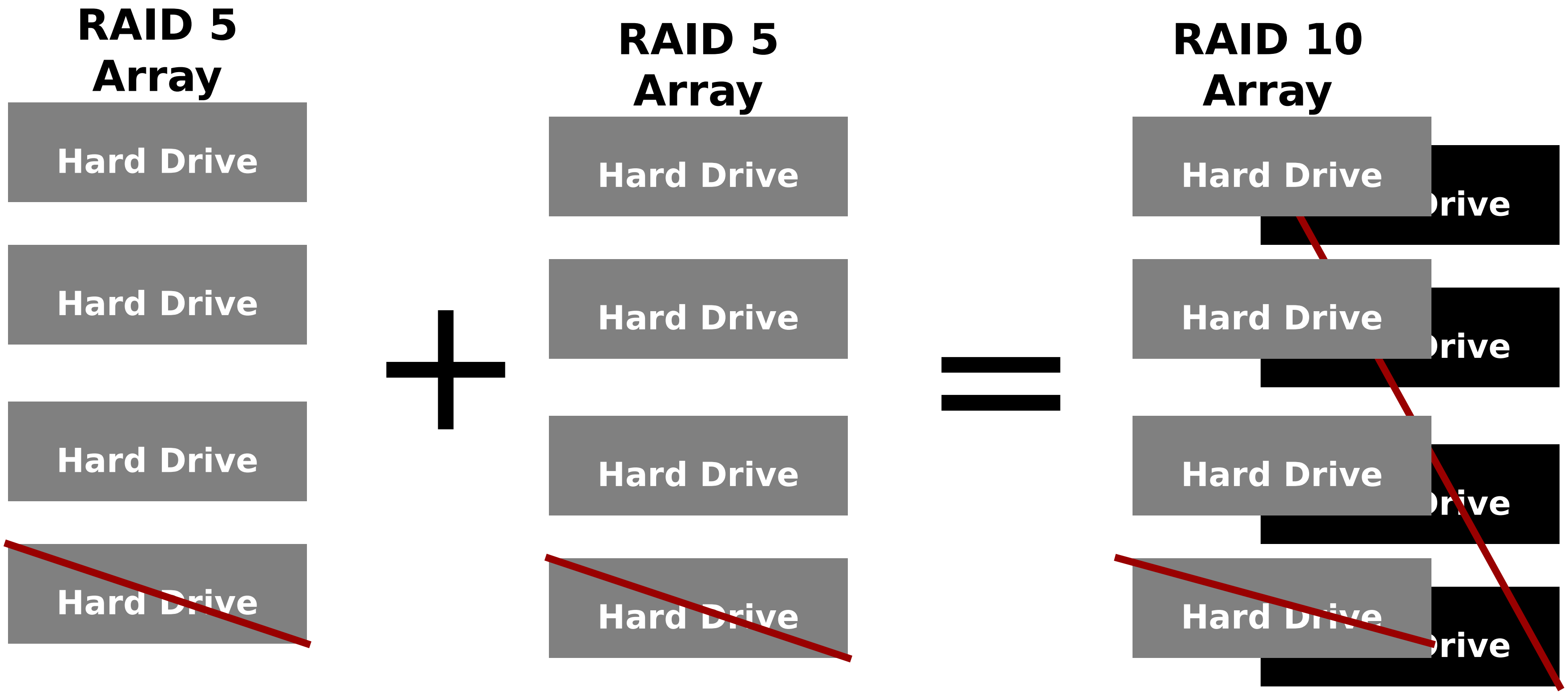
Disaster Recovery

Windows 2000 CD	To complete the restore
Computer Name	To put the computer back on the domain
Domain information	To put the computer back on the domain
IP Address (if static)	
Video Settings	These will be lost
Network settings	These too will have to be reset

Disaster Avoidance

- Consider a fault tolerant disk configuration
- Multiple DC’s
- Wins replication partners
- Backup DHCP servers
- Replicated data
- Clusters for servers that need to be highly available

RAID 5 and RAID 10



RAID 5 Array

Hard Drive

Hard Drive

Hard Drive

~~Hard Drive~~

+

RAID 5 Array

Hard Drive

Hard Drive

Hard Drive

~~Hard Drive~~

=

RAID 10 Array

Hard Drive

Drive

Hard Drive

Drive

Hard Drive

Drive

~~Hard Drive~~

Drive

Restore

- Do not use a Windows NT® 4 product
  - It will not work on new File types
  - It may fail silently
  - You will not be happy
- An exchange aware backup software is required to backup exchange properly
- Watch your backup logs and events

Disaster Recovery and Planning

- System State
- Time Frame for the inevitable
  - Backup time
  - Restore time
- Hard Drive Redundancy
- Server Protection
  - UPS

Disaster Recovery

Fix or replace broken hardware	Unknown
Install Windows 2000	90 minutes
Restore Full System from Tape	Depends on tape – 2-4 hours is reasonable
Reboot and review services	At least an hour
Restore Databases or Additional user	Depends on size

Disaster Recovery

Local Administrator Password	Frequently forgotten, will be restored. Domain admin password will not work
Disk configurations and signatures (in case of cluster)	Disk configuration will need to be rebuilt manually
A backup set	No tape? No restore!

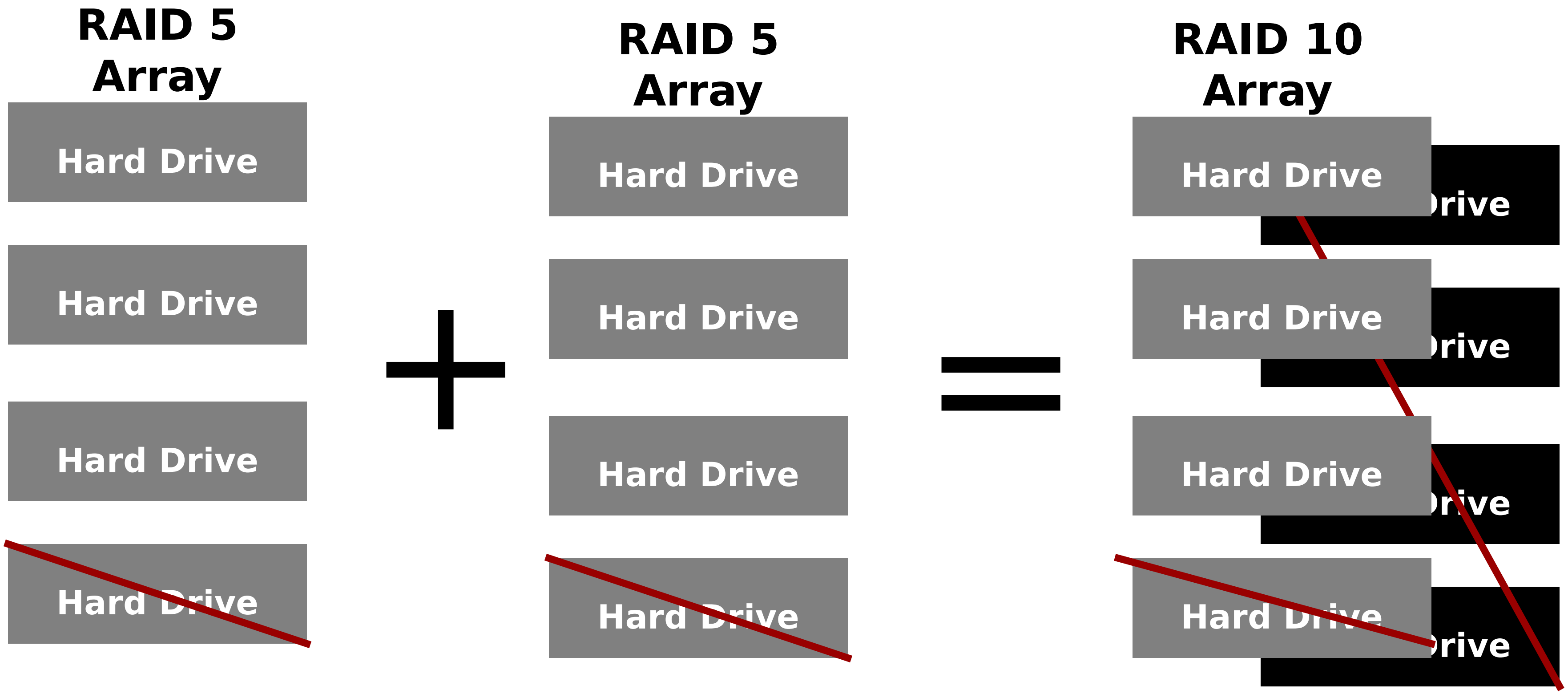
Disaster Recovery

Windows 2000 CD	To complete the restore
Computer Name	To put the computer back on the domain
Domain information	To put the computer back on the domain
IP Address (if static)	
Video Settings	These will be lost
Network settings	These too will have to be reset

Disaster Avoidance

- Consider a fault tolerant disk configuration
- Multiple DC’s
- Wins replication partners
- Backup DHCP servers
- Replicated data
- Clusters for servers that need to be highly available

RAID 5 and RAID 10



RAID 5 Array

Hard Drive

Hard Drive

Hard Drive

~~Hard Drive~~

+

RAID 5 Array

Hard Drive

Hard Drive

Hard Drive

~~Hard Drive~~

=

RAID 10 Array

Hard Drive

Hard Drive

Hard Drive

~~Hard Drive~~

rive

rive

rive

rive

Restore

- Do not use a Windows NT® 4 product
  - It will not work on new File types
  - It may fail silently
  - You will not be happy
- An exchange aware backup software is required to backup exchange properly
- Watch your backup logs and events

Authoritative Restore

- Authoritative

Active Directory	Used to roll back or “undo” mistaken changes
SysVol	Used to completely reset Sysvol
Replica sets	Used to roll back or “undo” changes to a

Primary Restore

- **Primary**

Active Directory	Used only to restore a standalone DC or the first of several DC’s
Sysvol	Used only to restore a standalone DC or the first of several DC’s
Replica Sets	Used to restore the first replica set only

Normal Restore

- Normal

Active Directory	Used in most cases to restore a DC in a replicated environment
Sysvol	Used in most cases to restore a DC in a replicated environment
Replica sets	Used to restore the 2nd-Nth replica sets

Restore

Active Directory	Boot into Active Directory (AD) maintenance mode if AD is running and restore AD, then mark authoritative by using NTDSUTIL tool
SysVol and Replica sets	Restore Sysvol to a temp location and then copy to the Sysvol Directory

Additional Resources

- Windows 2003 Help is very good and can assist with planning and best practices
- Books
- Internet
  - Google.com
    - Searches the web, technet and groups

Windows 2003 Summary

- Multiple flavors of 2003 server
- Active directory can be designed to reflect your organization using OU's
- GPO's can help you manage your domain
  - Much like NT policy's but a lot more powerful
- Three different types of Groups in Windows 2000
- The MMC is a powerful and customizable tool
- It is a good idea to run forest prep and domain prep on the first DC in your forest if you will ever think you will be running Exchange 2003
  - This way when the new DC's come on line they will replicate all of the schema changes when they come online.

Review Quiz

1. Q. What is the IP address that you will get if your computer is unable to contact a DHCP server? And what is this called?
2. Q. What is the order for granting permissions to an object?
3. Q. Which domain mode must you be in to use Universal groups?
4. Q. What is the port number for Terminal Services?
5. Q. How do you make a server into a Domain Controller?
6. Q. What is the default lease time for DHCP? When will the client attempt to renew?
7. Q.What are the three types of groups in Windows 2003?
8. Q. What is the biggest drawback of using the newest group in Windows 2003?

Terminal

Windows 2003

Managing Terminal Services

- How Terminal Services works
- How to set up Remote Administration mode
- How to set up Application Server mode
- How to set up Terminal Services licensing

What Is Terminal Services?

- Terminal Services gives Windows Server 2003 the ability to act as a *terminal server.*
- A terminal server uses a centralized computing model, rather than the distributed computing model you are probably accustomed to.
- Under the covers, Terminal Services works quite differently from products like pcAnywhere.
- Most remote control products only allow a single user to control the remote computer,
- Terminal Services is designed for multiple users

Terminal Services Capabilities

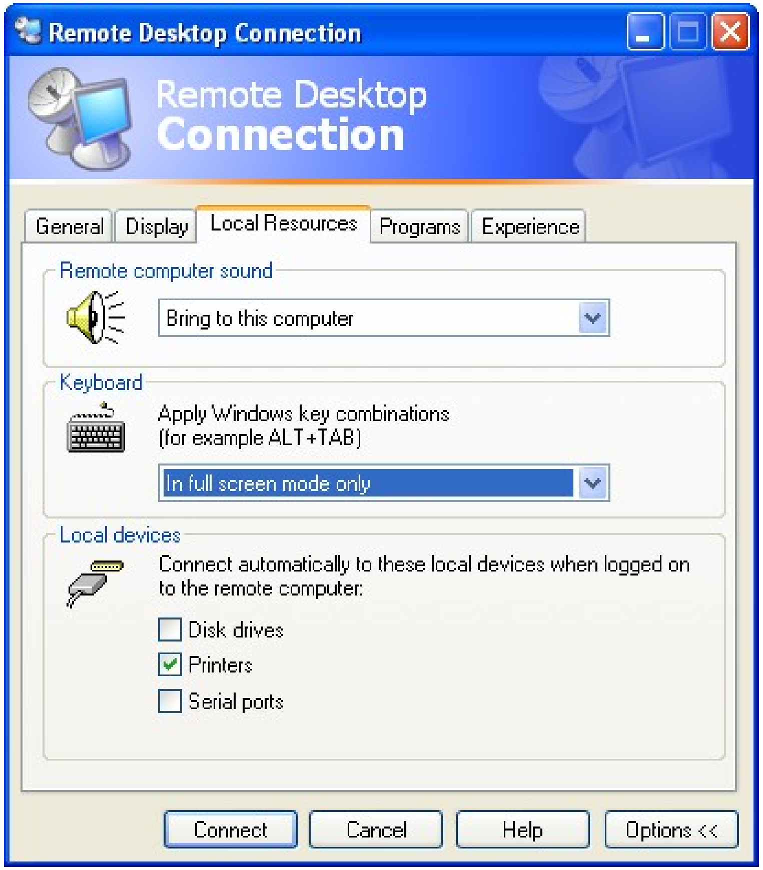
Applications can do all of the following tasks when running on a computer:

- Print documents to a print device that is attached to the computer
- Play sounds through the computer's speakers and sound card
- Access the storage devices, like hard disks and CD-ROM drives, on the computer
- Access the communications ports, such as serial ports, on the computer

When an application is running on a Terminal Services server, the application doesn't realize that it's being controlled by a user on a totally different computer.

- Documents print to the printer attached to the Terminal Services server, rather than to a printer that is physically close to the user.
- Sounds play on the server, not on the user's computer.
- Only the server's storage devices are accessible, although the user's documents might be on his computer instead of on the server.
- Only the server's communications ports are available, although the user might have devices attached to her client computer's communications ports.
- When a user connects to a Terminal Services server, the server attempts to create printers that match the printers configured on the user's client computer.

RDP



Remote Desktop Connection

Remote Desktop Connection

Remote computer sound

Bring to this computer

Keyboard

Apply Windows key combinations
(for example ALT+TAB)

In full screen mode only

Local devices

Connect automatically to these local devices when logged on to the remote computer:

☐ Disk drives

☑ Printers

☐ Serial ports

Why Use Terminal Services?

- Terminal Services is a great way for users to remotely work on company projects.
- running application has a full-speed local area network (LAN) connection, which can handle the data.

Remote Administration with Terminal Services

- Windows Server 2003 automatically installs Terminal Services in Remote Administration mode
  - Remote Administration mode enables members of the server's Administrators group to remotely control the server, just as if they were standing in front of it.
    - Up to two administrators can connect at once.

Application Server Mode

- Although Remote Administration mode is certainly useful, application server (also called *AppServer*) mode is where Terminal Services really shines. AppServer mode enables users to connect to Terminal Services and run applications.
- AppServer mode enables users to connect to Terminal Services and run applications.

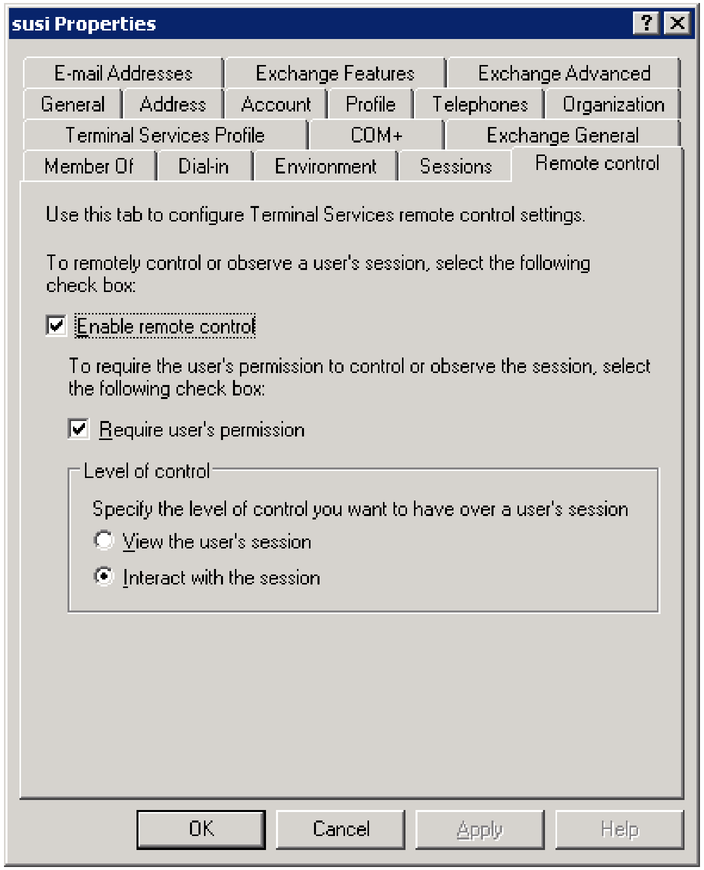
Setting up applications

- Applications running on a Terminal Services server have some restrictions on how they behave.
- Some applications, such as Microsoft Office XP, take special steps when you install them on a server that is running Terminal Services in AppServer mode.
  - **1.** Open a command-line window.
  - **2.** Type **change user /install** and press Enter.
  - **3.** Install the application using its regular Setup routine. Be sure to install the application on an NTFS volume.
  - **4.** Type **change user /execute** and press Enter.
  - **5.** Run any appropriate application compatibility scripts.

Setting up users

You can adjust the following properties on a per-user basis:

- Whether or not a user is permitted to log on to Terminal Services
- How long a user may remain connected once logged on
- How long the user may remain idle before Terminal Services disconnects him
- How long disconnected sessions remain active before Terminal Services logs the user off. A user can disconnect and then reconnect later, and her session will still be up and running. When a user logs off, her session is terminated.
- How many active sessions a single user may have at once.



Use this tab to configure Terminal Services remote control settings.

To remotely control or observe a user's session, select the following check box:

☑ Enable remote control

To require the user's permission to control or observe the session, select the following check box:

☑ Require user's permission

Level of control

Specify the level of control you want to have over a user's session

○ View the user's session

● Interact with the session

Terminal Services Licensing

- You can install Terminal Services Licensing on any Windows Server 2003. Simply follow the same procedure for installing Terminal Services:
  - Open Add/Remove Programs,
  - click on Add/Remove Windows Components, and place a checkmark next to Terminal Services Licensing
- Licensing servers keep track of how many Terminal Services Licenses you have purchased.
- When your company purchases Terminal Services licenses, you must activate those licenses using Microsoft's Web site and the Terminal Services Licensing application, which is installed on Licensing servers.

REVIEW

You learned how Terminal Services works, and how it can be used in an enterprise environment. You learned how to install Terminal Services in AppServer mode, and how to use Terminal Services for remote server administration. You also learned about Terminal Services licensing, and how to install applications on a Terminal Services server running in AppServer mode.

SERVICES

Managing the Dynamic Host Configuration Protocol

- How the Dynamic Host Configuration Protocol works
- How to install and configure the Dynamic Host Configuration Protocol
- How to manage the Dynamic Host Configuration Protocol

The settings can include:

- The IP address of one or more DNS servers
- The IP address of one of more WINS servers
- The IP address of the default gateway
- The domain name that client computers should use

How DHCP Works

DHCP is a client-server process

1. When the client computer starts, it realizes that it doesn’t have an IP address or other IP settings but is instead configured to use DHCP.

2. The client computer broadcasts a DHCP request packet. All computers on the local subnet receive the broadcast, but only a DHCP server recognizes the request and processes it.

3. The DHCP server selects an available IP address from its database. The address matches the subnet that the DHCP request came from, ensuring that the client will be able to use the address.

Continue.

4. The DHCP server sends a DHCP offer packet to the client’s physical address. The offer includes the IP address the DHCP server selected, as well as other configuration information, like the IP addresses of the DNS server that the client should use.

5. The DHCP client acknowledges receipt of the IP configuration information and begins using the new settings. The IP address the client received is *leased* from the DHCP server for a specific period of time.

6. When 50 percent of the lease time has expired, the DHCP client sends a DHCP renew packet to the DHCP server. The server renews the DHCP lease, allowing the client to continue using the IP configuration it already has, without performing another DHCP request.

Default Installed Services

- Client for Microsoft Networks
  - Equivilent to the workstation service
  - Enables 2003 computers to access files/printers located on other computers across the network
- File & Printer Sharing for MS Networks
  - Equivilent to the server service
  - Enables 2003 computer to share its files and printers with other computers on the network

Dynamic Host Configuration Protocol

- Assigns automatic TCP/IP configuration remains unchanged
- Create scope/lease via DHCP Snap-in (part of DHCP service install)
- Scope must be activated before clients can receive configuration
  - Install DCHP Service on either domain controller or stand-alone server
  - Server configured with static IP address, subnet mask and default gateway

Administer/Authorize the Server

- DHCP Snap-in or DCHP located in Computer Management
- DHCP server must be authorized within Active Directory to provide services
- To authorize
  - Use DCHP snap-in added to your MMC
  - Right-click DHCP server name
  - Click Authorize
  - Right click the server and click Refresh
  - It should reflect a green up arrow if authorized

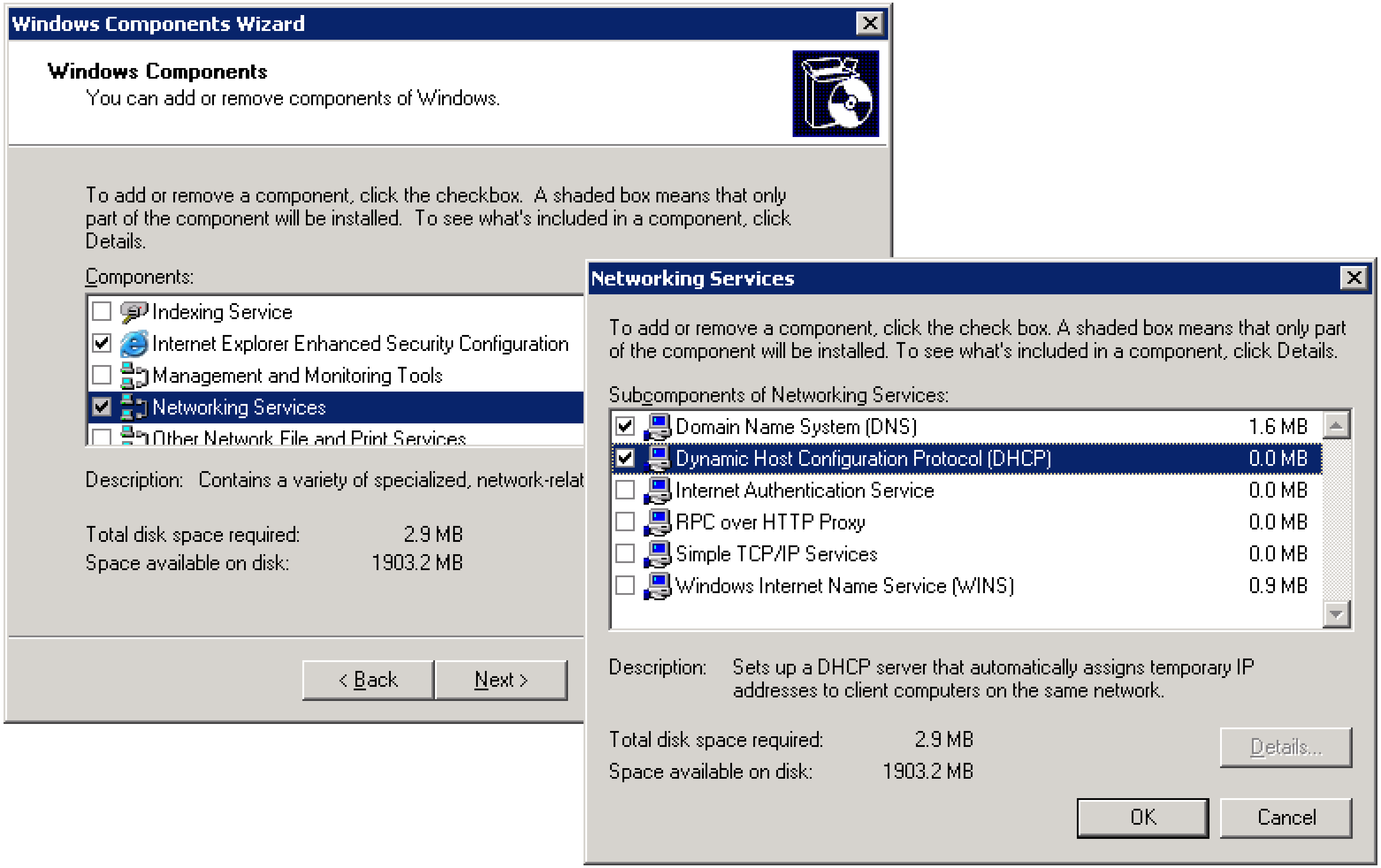
Guidelines for Creating Scope

- At least one scope for every DHCP server
- Exclude static IP addresses such as DHCP server, routers
- Create multiple scopes and assign only one scope to a specific subnet
- Same IP addresses should not exist in more than one scope
- Configure scope name, description, IP address range, subnet mask, excluded IP addresses, lease duration and any options

Steps -- Add Network Service DCHP

- Add DHCP to a server via the Control Panel, Add/Remove Programs utility
- Click Add/Remove Windows Components
- Click Networking Services (not the check box)
- Click Details and select DHCP
- Once the service is loaded, it is started automatically

Installing DHCP



Windows Components Wizard

Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

- ☐ Indexing Service
- ☑ Internet Explorer Enhanced Security Configuration
- ☐ Management and Monitoring Tools
- ☑ Networking Services
- ☐ Other Network File and Print Services

Description: Contains a variety of specialized, network-relat

Total disk space required:	2.9 MB
Space available on disk:	1903.2 MB

Networking Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

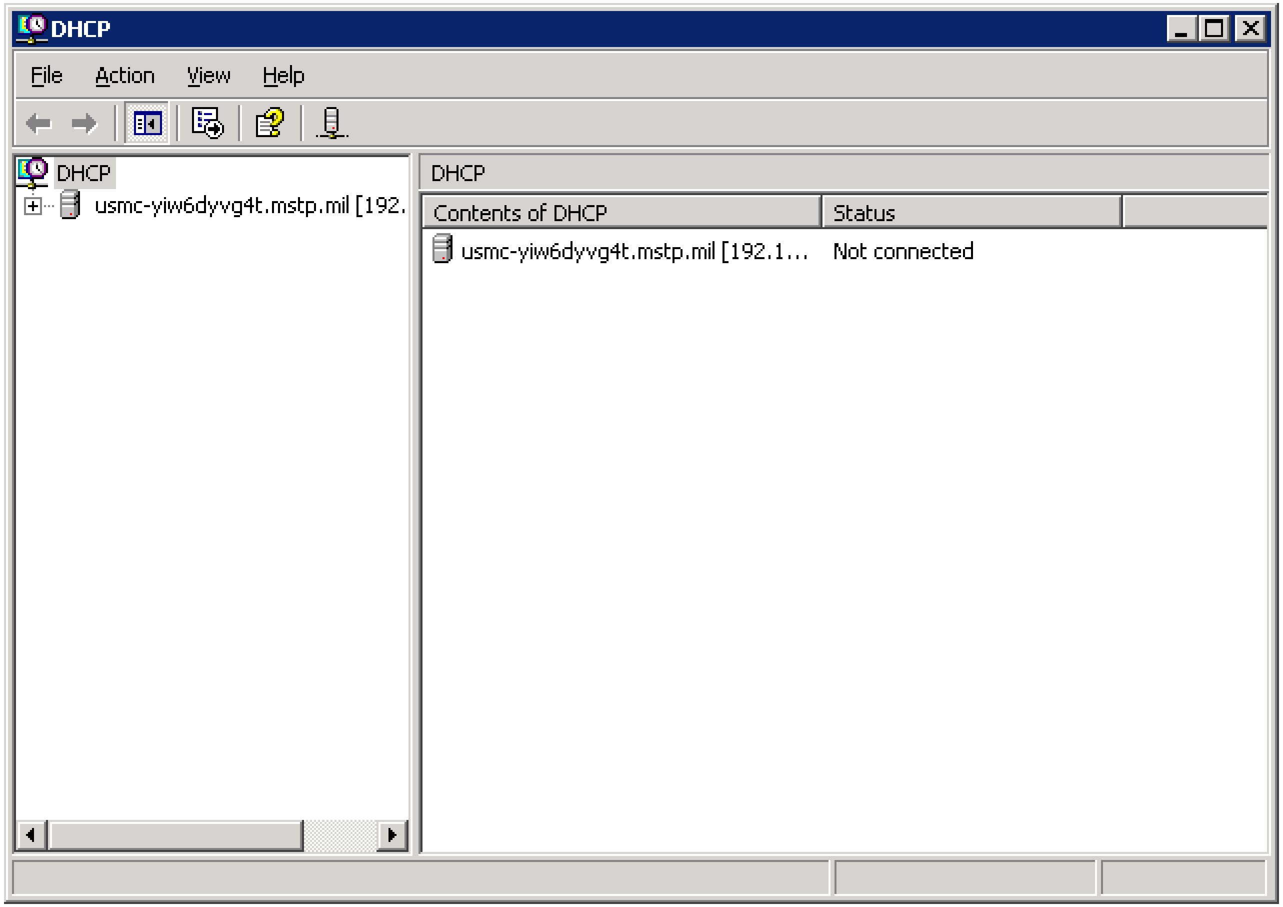
Subcomponents of Networking Services:

☑	Domain Name System (DNS)	1.6 MB
☑	Dynamic Host Configuration Protocol (DHCP)	0.0 MB
☐	Internet Authentication Service	0.0 MB
☐	RPC over HTTP Proxy	0.0 MB
☐	Simple TCP/IP Services	0.0 MB
☐	Windows Internet Name Service (WINS)	0.9 MB

Description: Sets up a DHCP server that automatically assigns temporary IP addresses to client computers on the same network.

Total disk space required:	2.9 MB
Space available on disk:	1903.2 MB

DHCP console



Contents of DHCP	Status
usmc-yiw6dyvg4t.mstp.mil [192.1...	Not connected

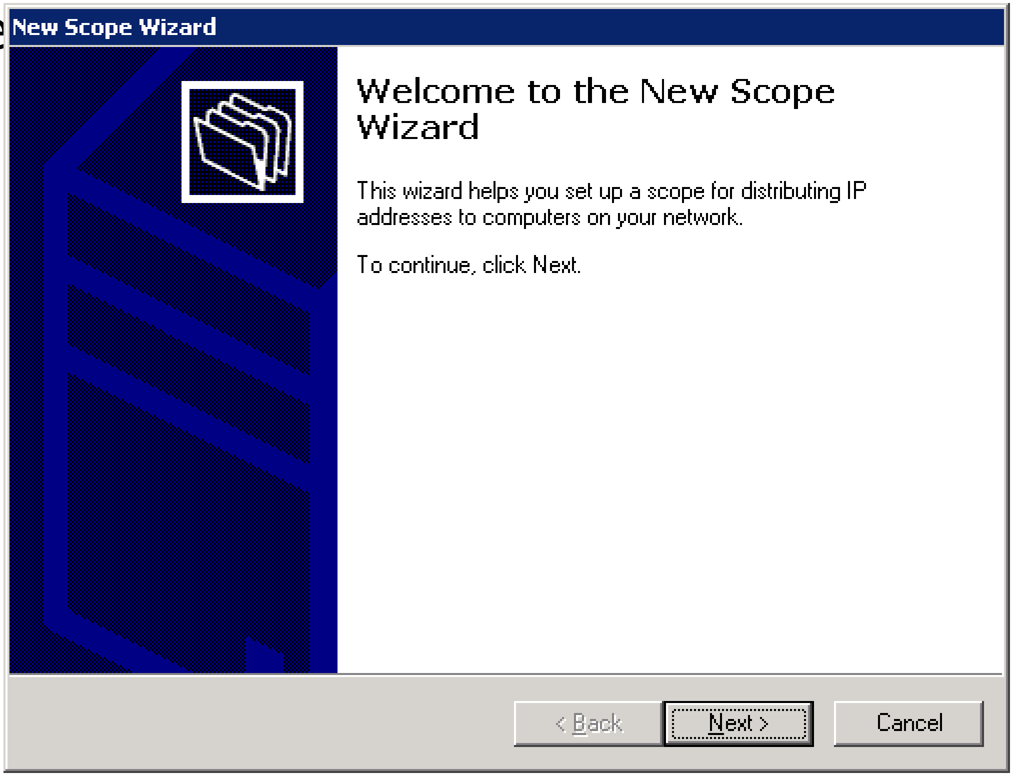
Setting an initial DHCP configuration

Your DHCP server's initial configuration should include the

- **One or more *scopes*.** Each scope represents a single subnet on your network and includes a range of IP addresses that are valid on that subnet.
- **One or more *server options*.** Each option configures a specific TCP/IP setting, such as the IP address of your DNS server.
- **One or more *scope options.*** Each option configures a specific TCP/IP setting, such as the IP address of a subnet's default gateway

Create a DHCP Scope

- Click the DHCP Server name
- From DHCP snap-in Action menu select New Scope to launch New Scope
- Click Next



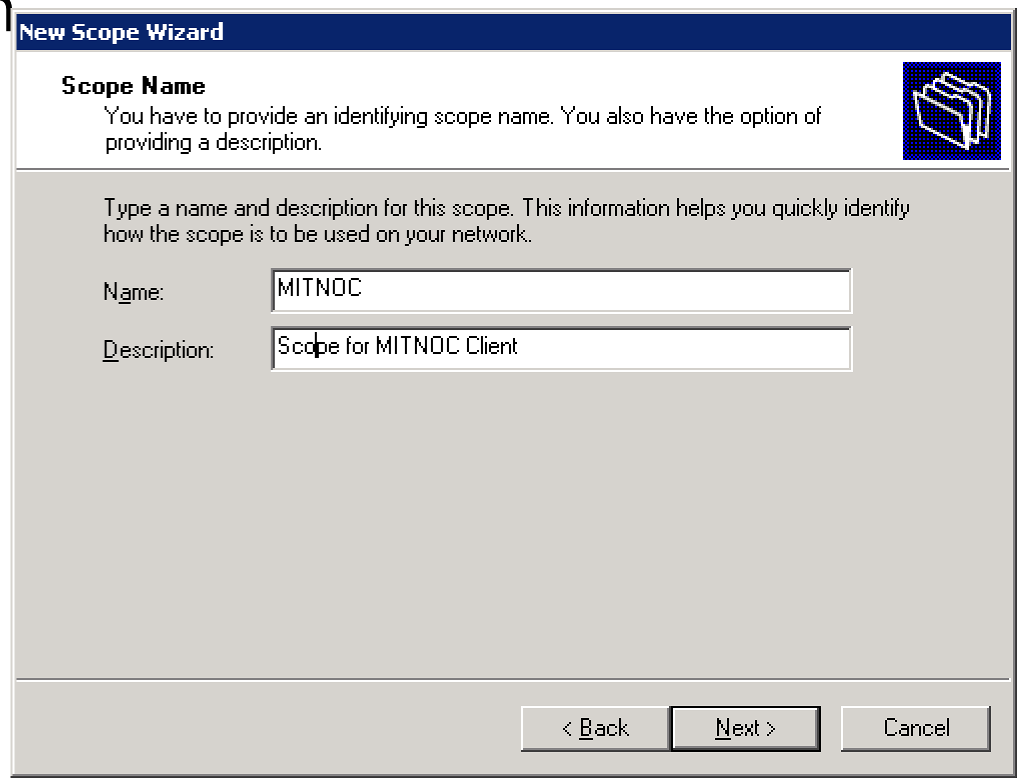
Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

Scope Name Dialog Box

- Specify name that describes purpose of scope and a description
- Click Next



Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.

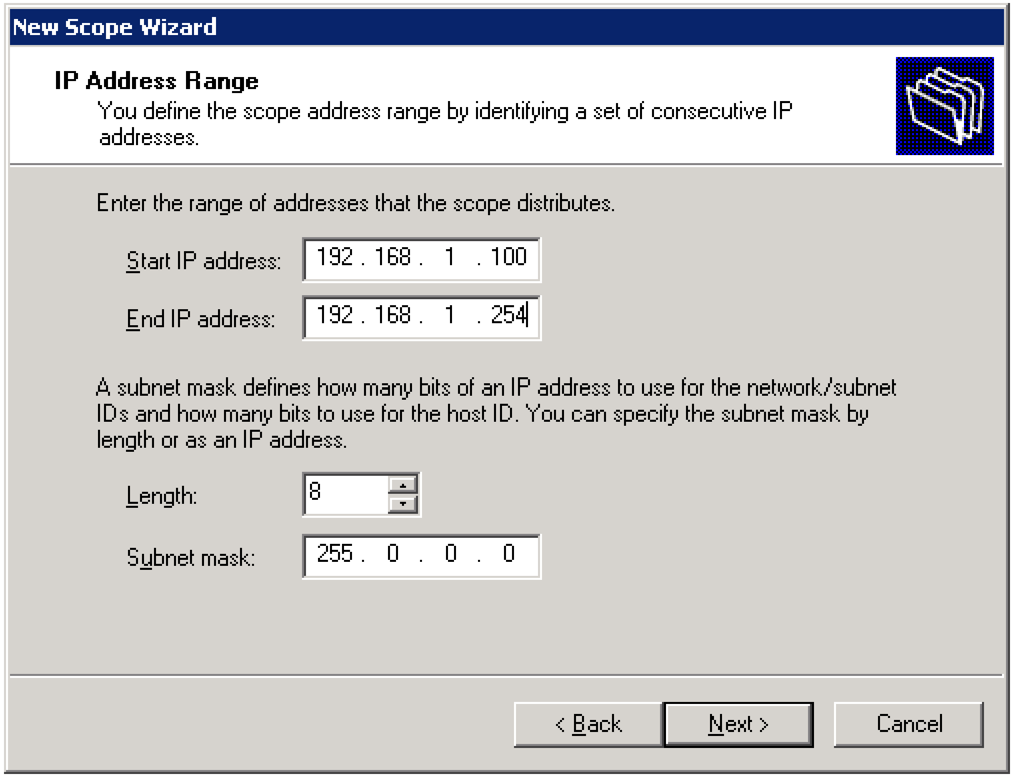
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: MITNOC

Description: Scope for MITNOC Client

IP Range Dialog Box

- Specify start IP address & ending IP address
- Subnet mask filled in once type start IP appropriate to class of IP
  - Change length if subnetting and click Next



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 1 . 100

End IP address: 192 . 168 . 1 . 254

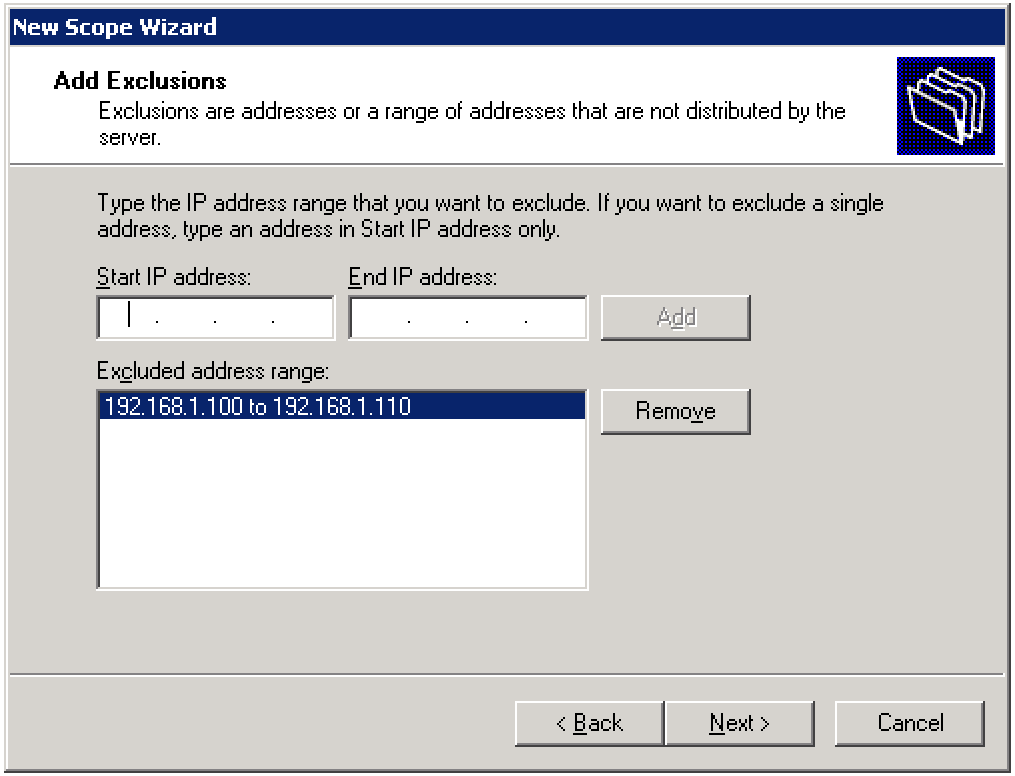
A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 8

Subnet mask: 255 . 0 . 0 . 0

Static Assigned IP -- Exclusions

- Specify addresses statically assigned to devices on subnet either a range or single IP addresses and click Add
- Click Next



New Scope Wizard

Add Exclusions

Exclusions are addresses or a range of addresses that are not distributed by the server.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: . . .

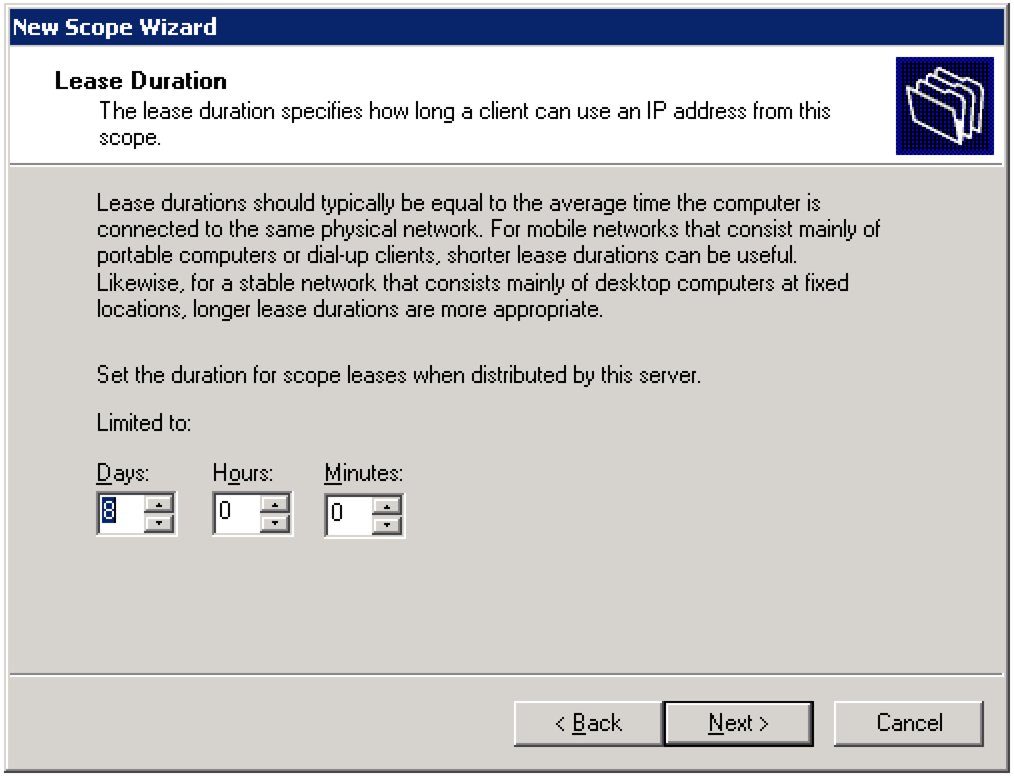
End IP address: . . .

Excluded address range:

192.168.1.100 to 192.168.1.110

Lease Duration

- Specify number of days, hours or minutes IP assigned to client; default is 8 days
- If ISP, would change the default



New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

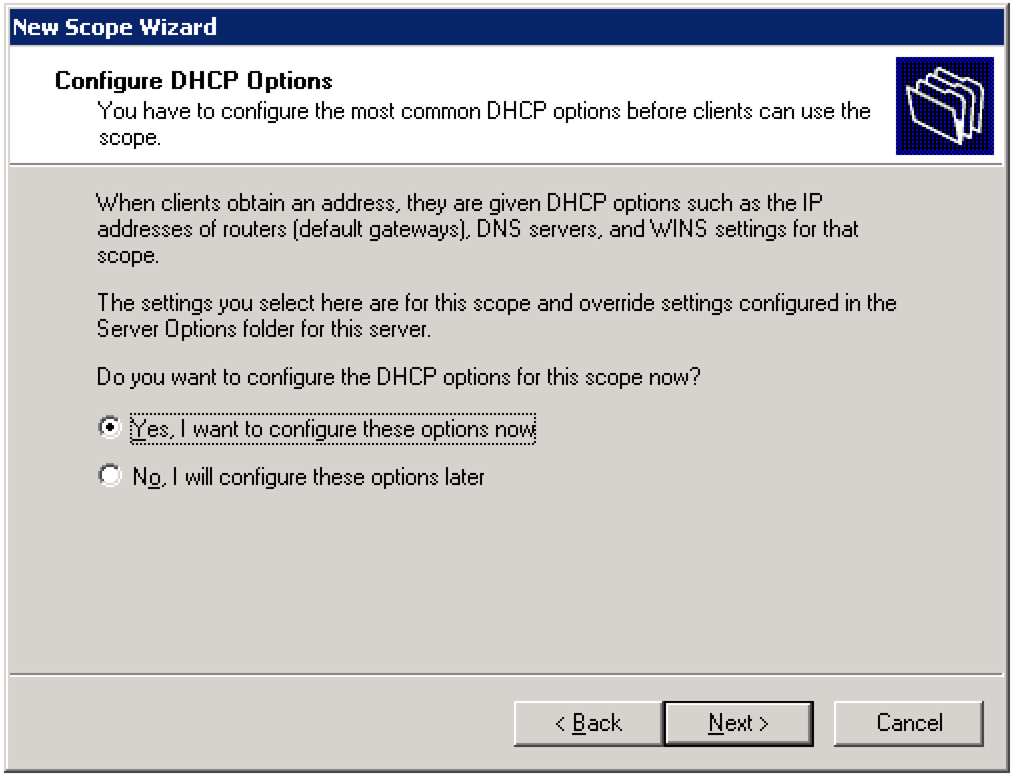
Set the duration for scope leases when distributed by this server.

Limited to:

Days: 8 Hours: 0 Minutes: 0

DHCP Options

- If desire to configure a gateway, DNS server or WINS server to be assigned to DHCP clients, specify Yes for additional options



New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

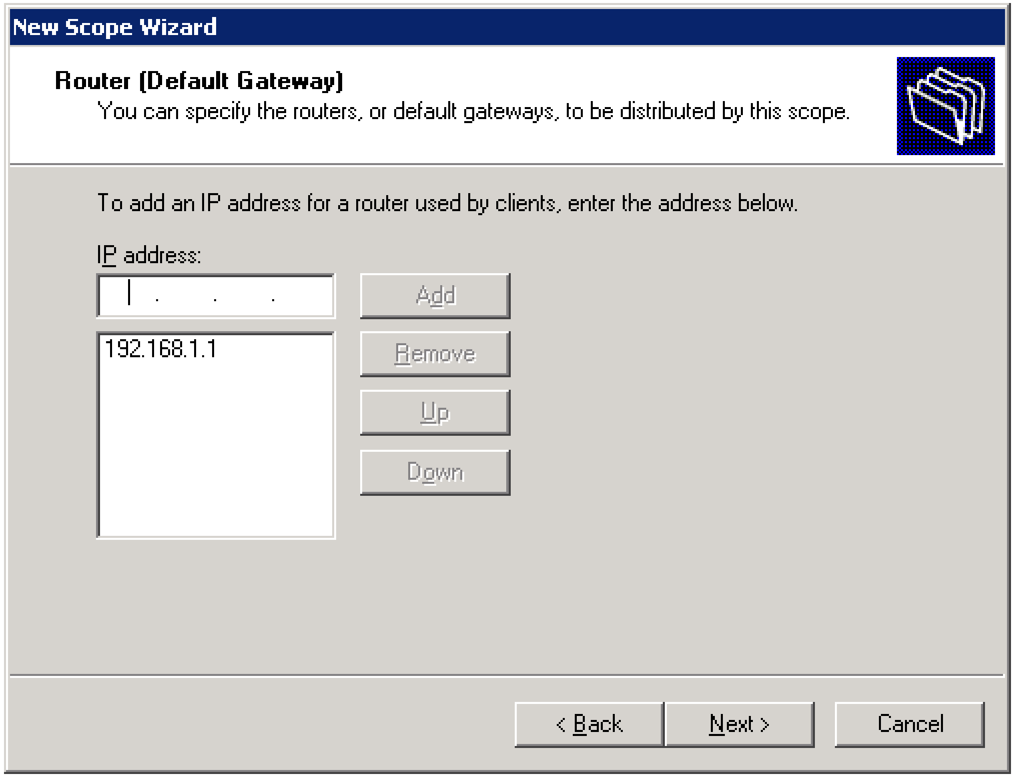
Do you want to configure the DHCP options for this scope now?

● Yes, I want to configure these options now

○ No, I will configure these options later

Gateway Dialog Screen

- Specify IP address of gateway, typically a router to get outside your network
- This is the 003 Router record



New Scope Wizard

Router (Default Gateway)

You can specify the routers, or default gateways, to be distributed by this scope.

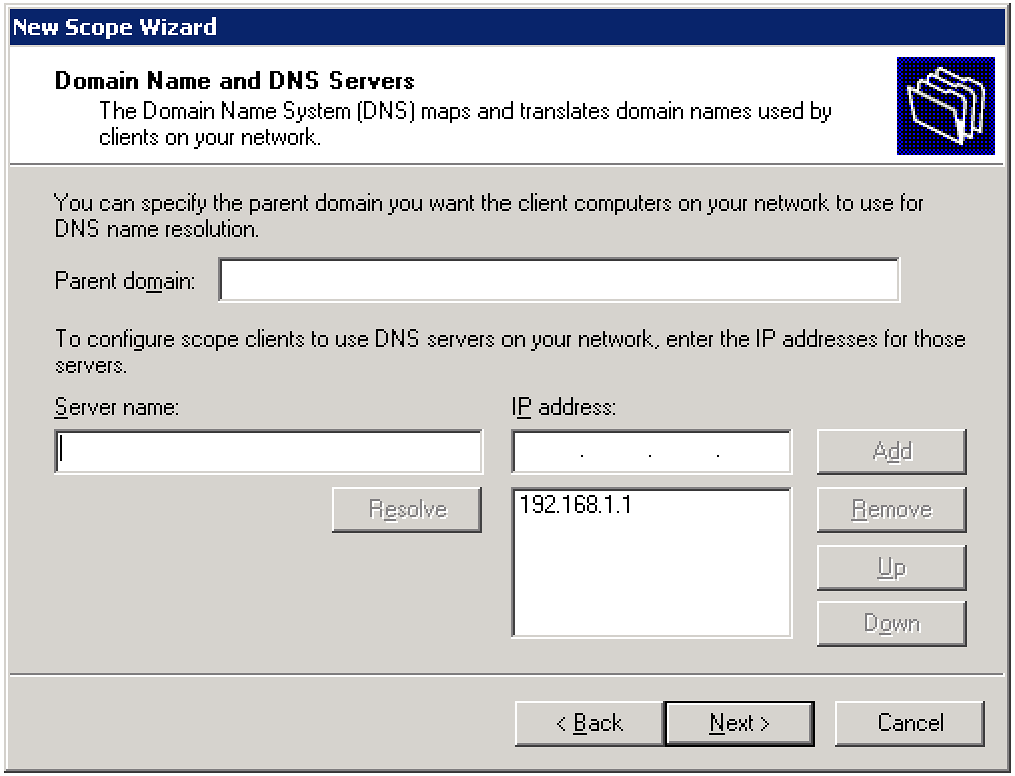
To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.1.1

DNS Dialog Screen

- Specify IP address of the DNS server
- Can specify Server name and click Resolve
- Click Add
- Click Next



New Scope Wizard

Domain Name and DNS Servers

The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

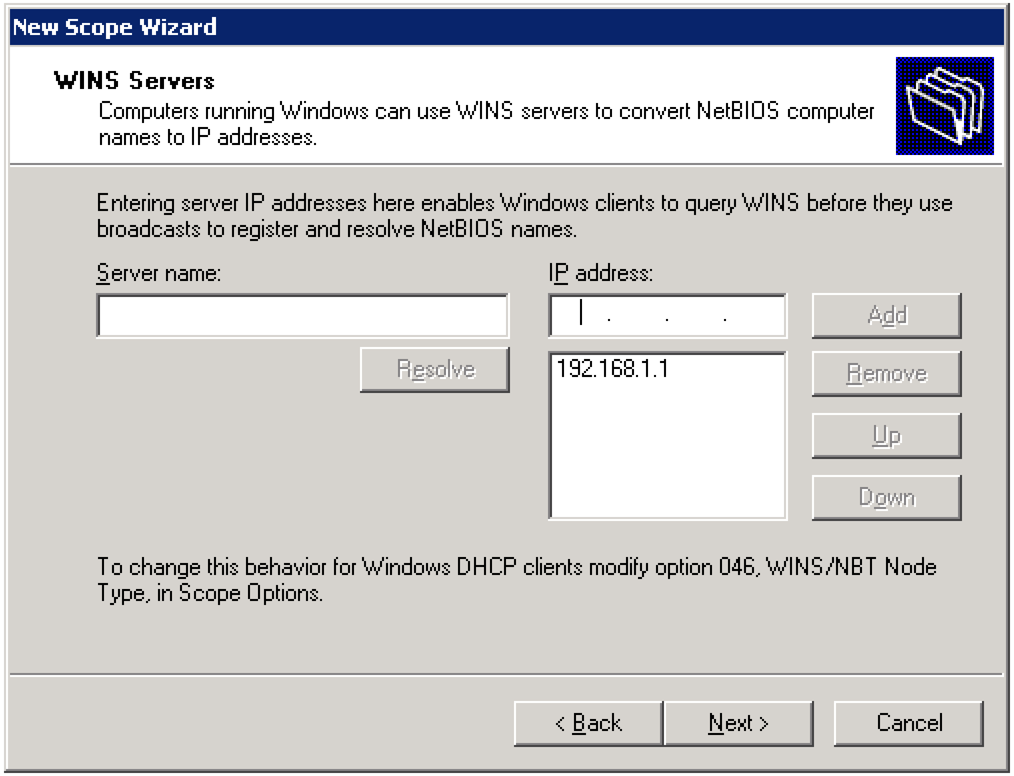
Server name:

IP address:

192.168.1.1

WINS Dialog Screen

- Specify IP address of WINS server for legacy clients
- Can specify Server name and click Resolve
- Click Add
- Click Next



New Scope Wizard

WINS Servers

Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

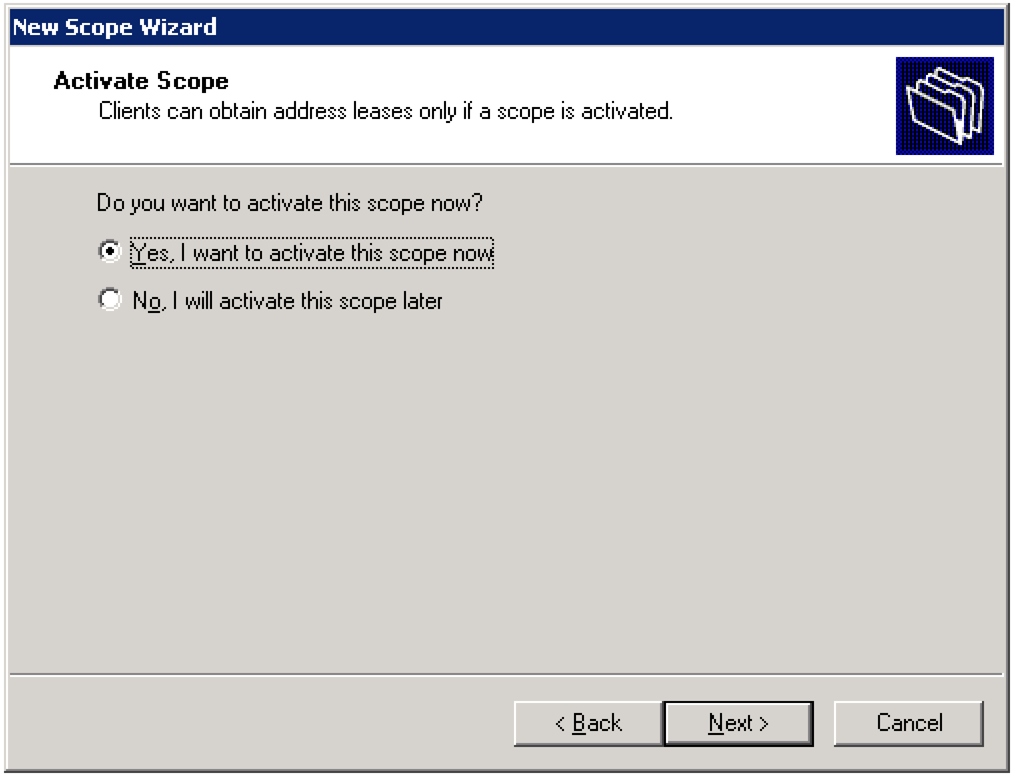
Server name:

IP address: 192.168.1.1

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

Activate the Scope

- Asked to activate the scope
- In order to use scope, it must be activated
- Click Next



New Scope Wizard

Activate Scope

Clients can obtain address leases only if a scope is activated.

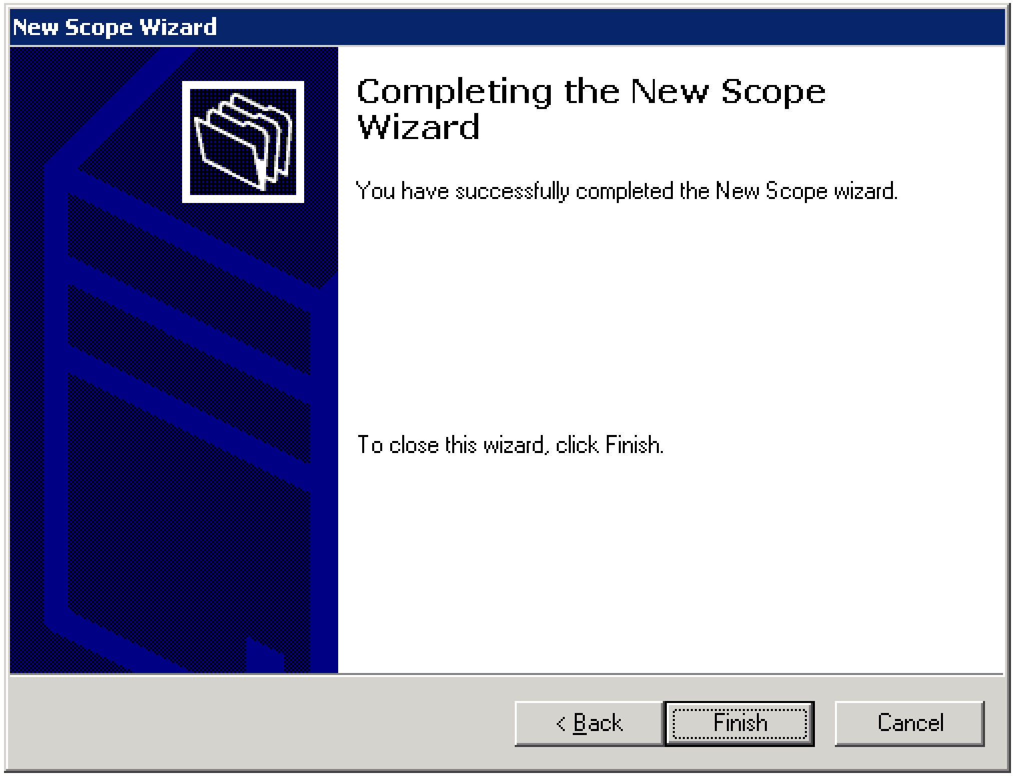
Do you want to activate this scope now?

● Yes, I want to activate this scope now

○ No, I will activate this scope later

DHCP Scope Complete

- Click Finish to complete the Scope Wizard



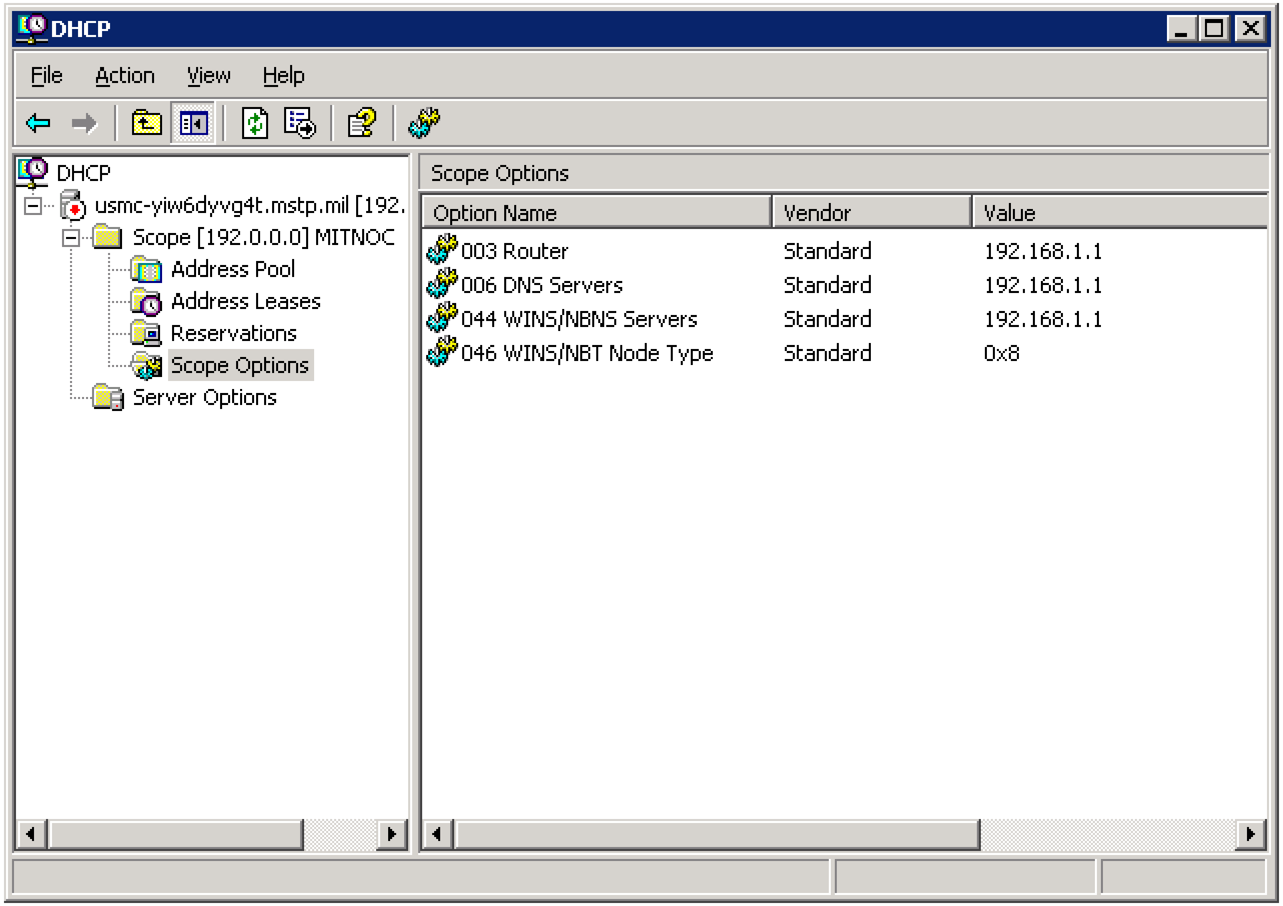
Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

To close this wizard, click Finish.

Changing a DHCP Scope

- To change range or lease parameters bring up the scope properties
- To change exclusions, right-click the scope and access Address Pool
- To change options, right-click the scope option and click Configure Options. Click the option needed to be changed



Option Name	Vendor	Value
003 Router	Standard	192.168.1.1
006 DNS Servers	Standard	192.168.1.1
044 WINS/NBNS Servers	Standard	192.168.1.1
046 WINS/NBT Node Type	Standard	0x8

Automatic Private IP Addressing

- APIPA supports automatic address assignment of IP addresses for simple LAN-based network configurations
- Extension of dynamic IP assignment without configuring static IP or using DHCP service
- To function configure network clients for “Obtain an IP Address Automatically” in the TCP/IP properties

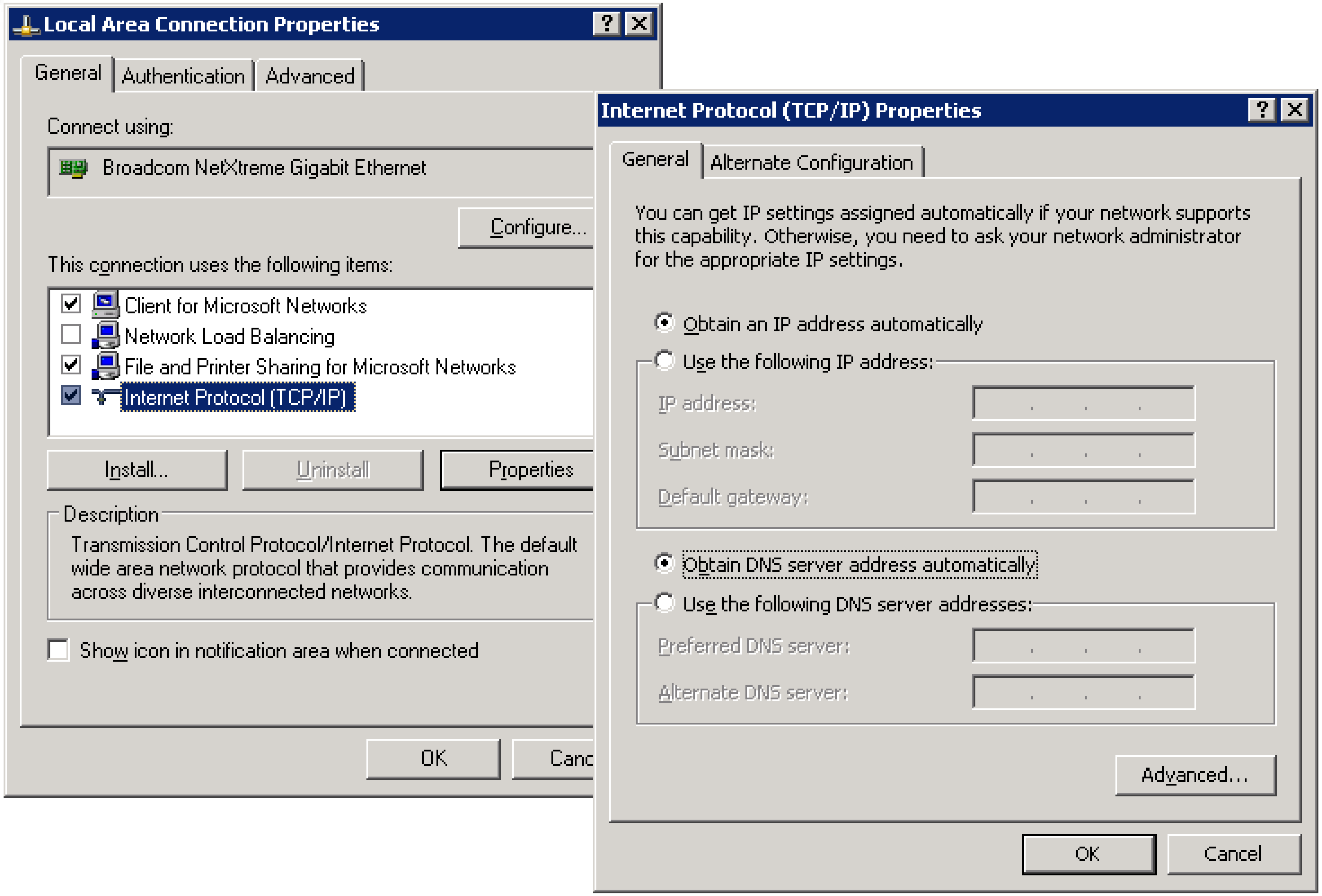
APIPA Assigning Addresses

- 2003 TCP/IP client attempts to find DHCP
- Can’t find DHCP server, no IP address is obtained
- APIPA generates an IP address of 169.254.x.y (client’s unique identifier) & subnet mask of 255.255.0.0 only
- If address in use, APIPA reselects an address up to 10 times
- 169.254.0.0 – 169.254.255.255 designated range for APIPA

APIPA Process Continues

- Computer broadcasts address and assigns the address to itself
- APIPA continues in use until DHCP Server sends configuration
- With APIPA, only computers on same subnet can communicate
- APIPA enabled by default; disable via registry edit of the value

Configuring clients to use DHCP



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Broadcom NetXtreme Gigabit Ethernet

This connection uses the following items:

- ☑ Client for Microsoft Networks
- □ Network Load Balancing
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

REVIEW

You learned about DHCP, the Dynamic Host Configuration Protocol. You learned how DHCP clients work with a DHCP server to obtain IP addresses and configuration settings, and how to manage a DHCP server using the DHCP console. You learned how to configure a DHCP server and DHCP clients, and you learned how to create DHCP reservations for computers that always need to have the same IP address. You also learned basic troubleshooting steps to help resolve DHCP problems.

MAGTF STAFF TRAINING PROGRAM

DOCEMUS PRIMAM ACIEM

Security Configuration Management

SCM

Using the Security Configuration Manager

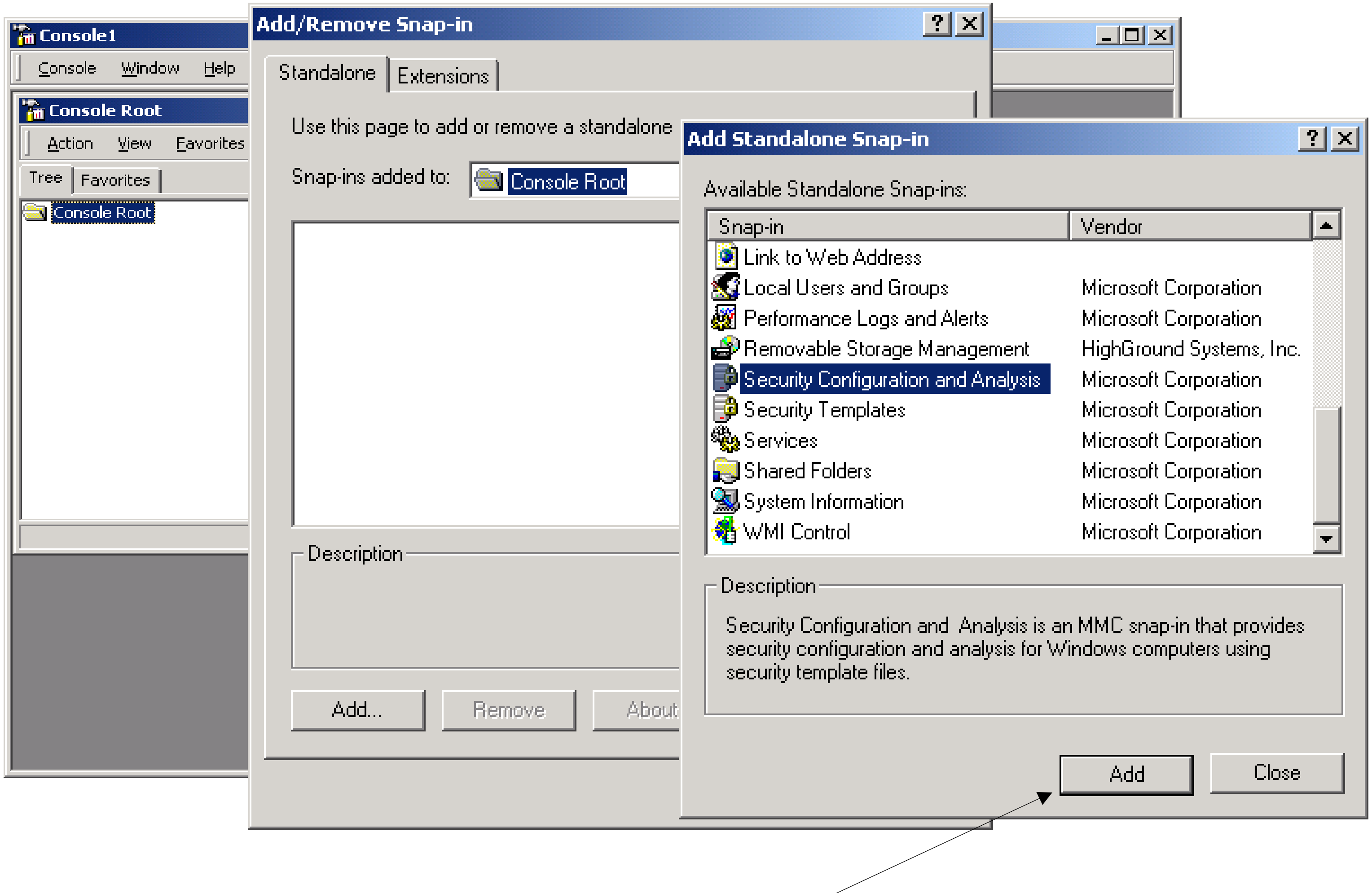
- How the Security Configuration Manager works, and what it’s used for
- How to manage server and domain security with the Security Configuration Manager
- How to create and use security templates

About the SCM

- The SCM is designed to analyze a computer and check its compliance with a given security template, apply a security template to a computer, or create a new security template based on a computer’s policy settings.
- The SCM also includes a command-line utility, **Secedit.exe**,

Opening the SCM

- The SCM is a collection of tools, which are available as Microsoft Management Console (MMC) snap-ins.



Use this page to add or remove a standalone

Snap-ins added to: Console Root

Description

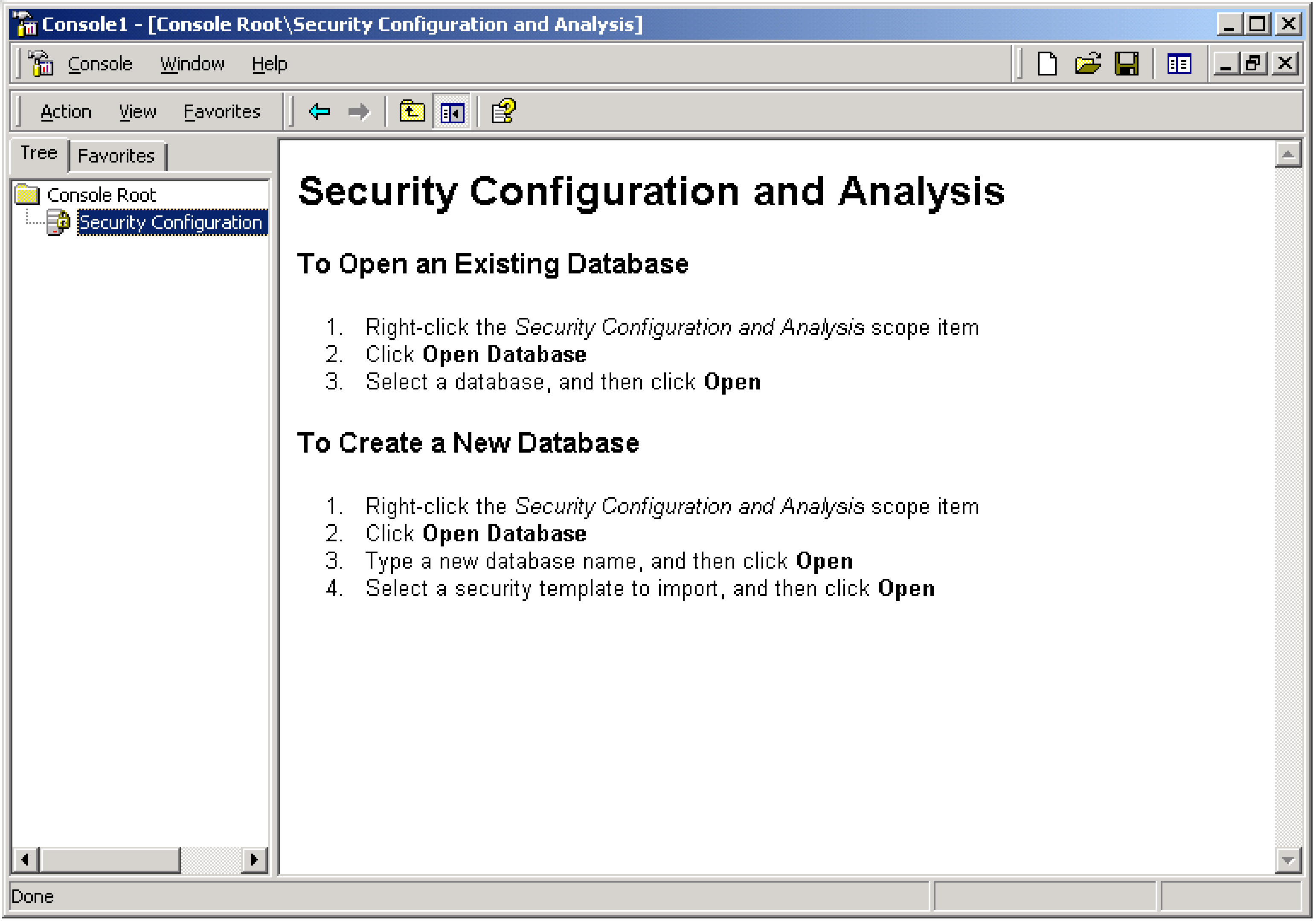
Available Standalone Snap-ins:

Snap-in	Vendor
Link to Web Address	
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Removable Storage Management	HighGround Systems, Inc.
Security Configuration and Analysis	Microsoft Corporation
Security Templates	Microsoft Corporation
Services	Microsoft Corporation
Shared Folders	Microsoft Corporation
System Information	Microsoft Corporation
WMI Control	Microsoft Corporation

Description

Security Configuration and Analysis is an MMC snap-in that provides security configuration and analysis for Windows computers using security template files.

Working with the SCM



Security Configuration and Analysis

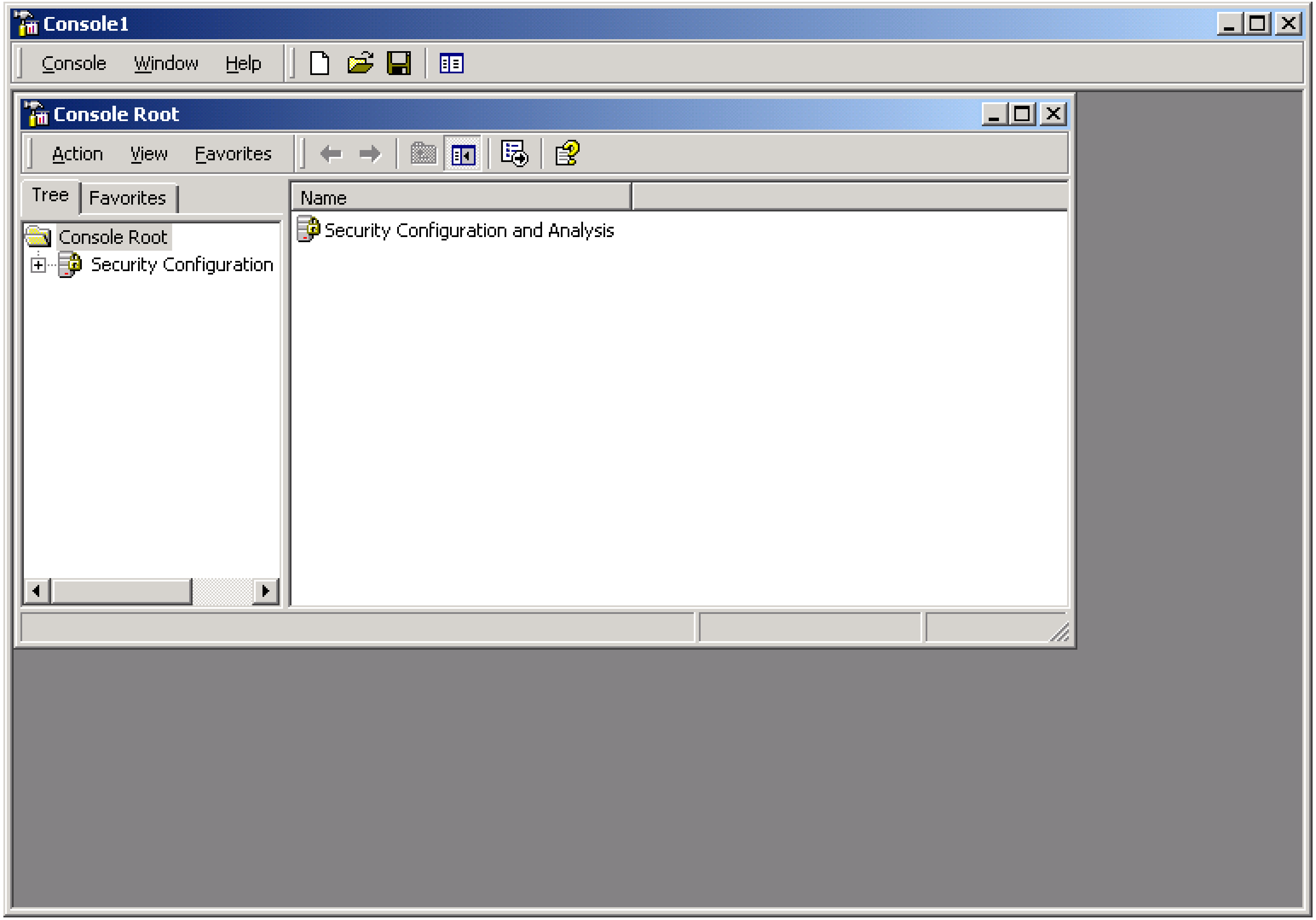
To Open an Existing Database

1. Right-click the *Security Configuration and Analysis* scope item
2. Click **Open Database**
3. Select a database, and then click **Open**

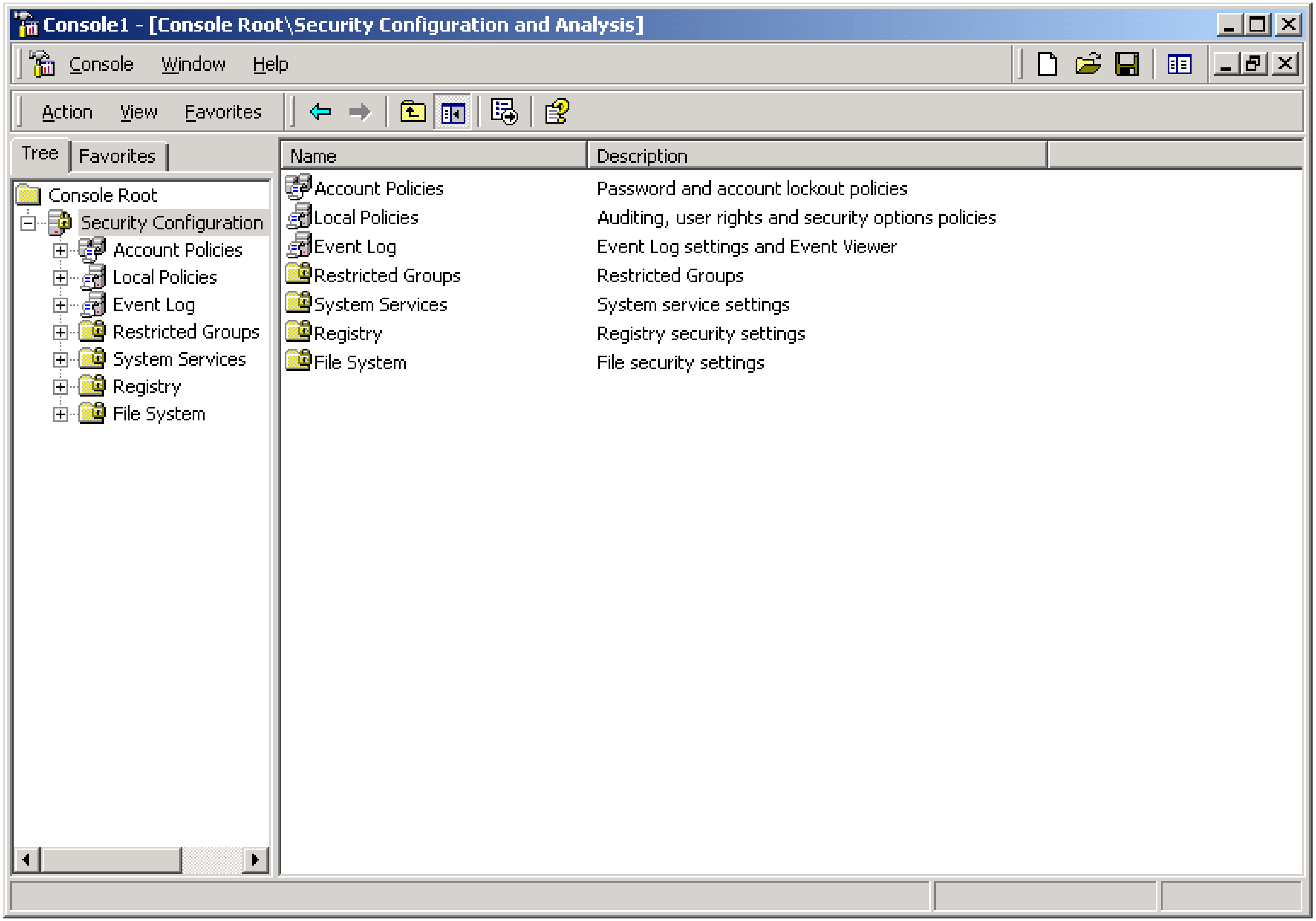
To Create a New Database

1. Right-click the *Security Configuration and Analysis* scope item
2. Click **Open Database**
3. Type a new database name, and then click **Open**
4. Select a security template to import, and then click **Open**

Working with the SCM



Working with the SCM

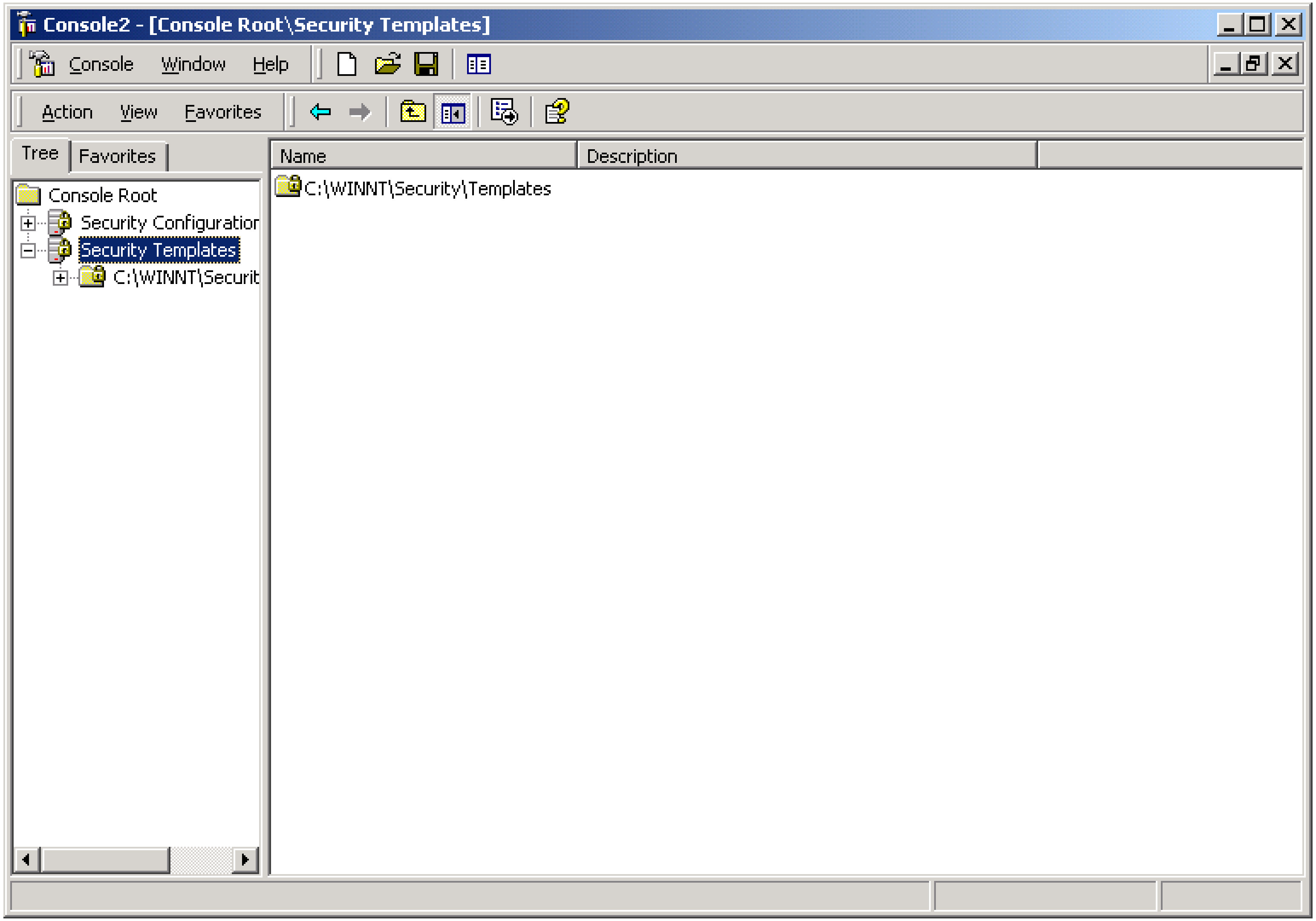


Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options policies
Event Log	Event Log settings and Event Viewer
Restricted Groups	Restricted Groups
System Services	System service settings
Registry	Registry security settings
File System	File security settings

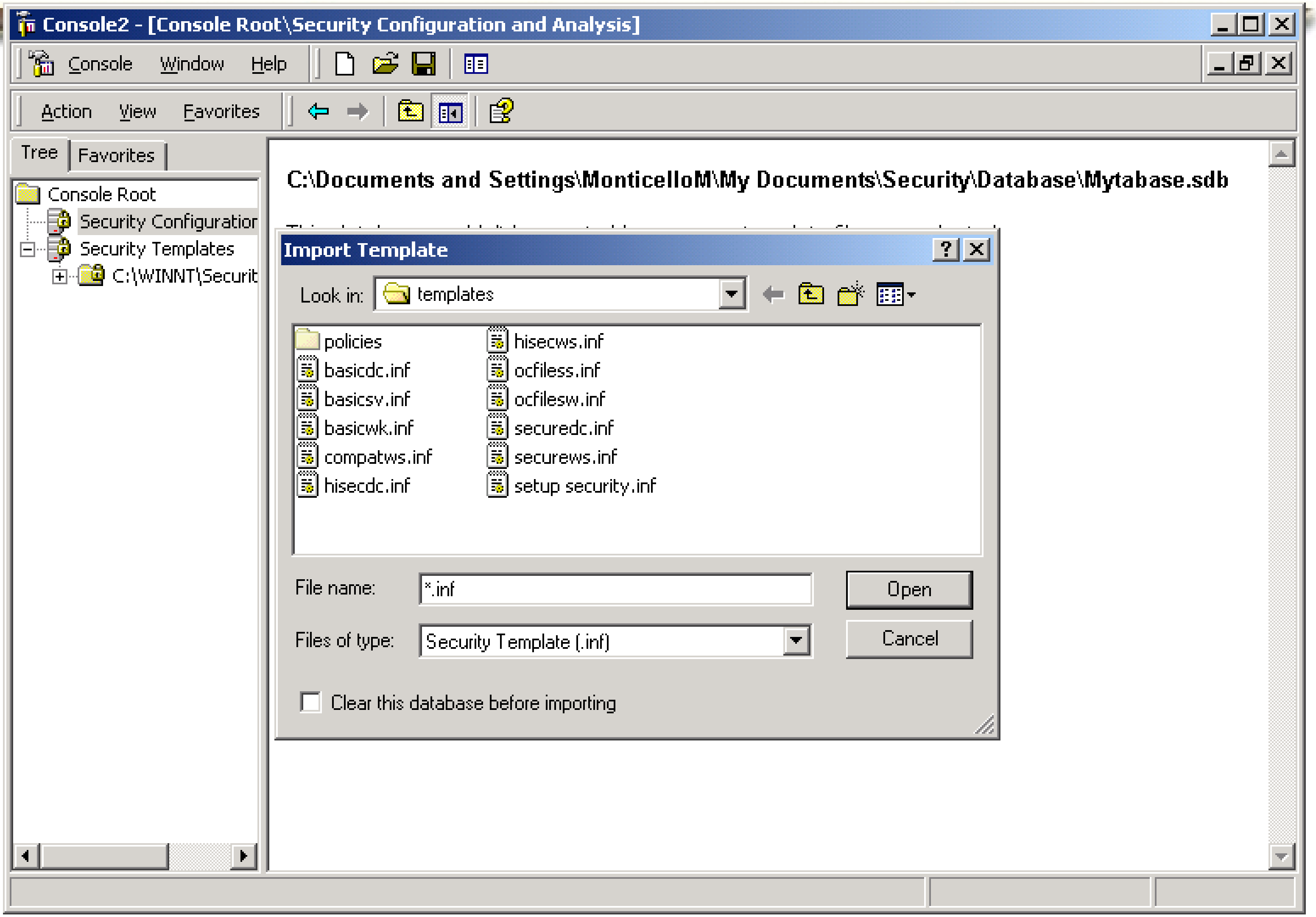
Security Templates

- Security templates enable you to create standardized security policies for your computers, and then easily apply those settings to a group of computers, either using “Security Configuration and Analysis,” **Secedit.exe**, or group policies. Microsoft provides several predefined security templates, and you can modify these or create your own.
- See next slide:

Security Templates



Predefined templates



C:\Documents and Settings\MonticelloM\My Documents\Security\Database\Mytabase.sdb

Look in: templates

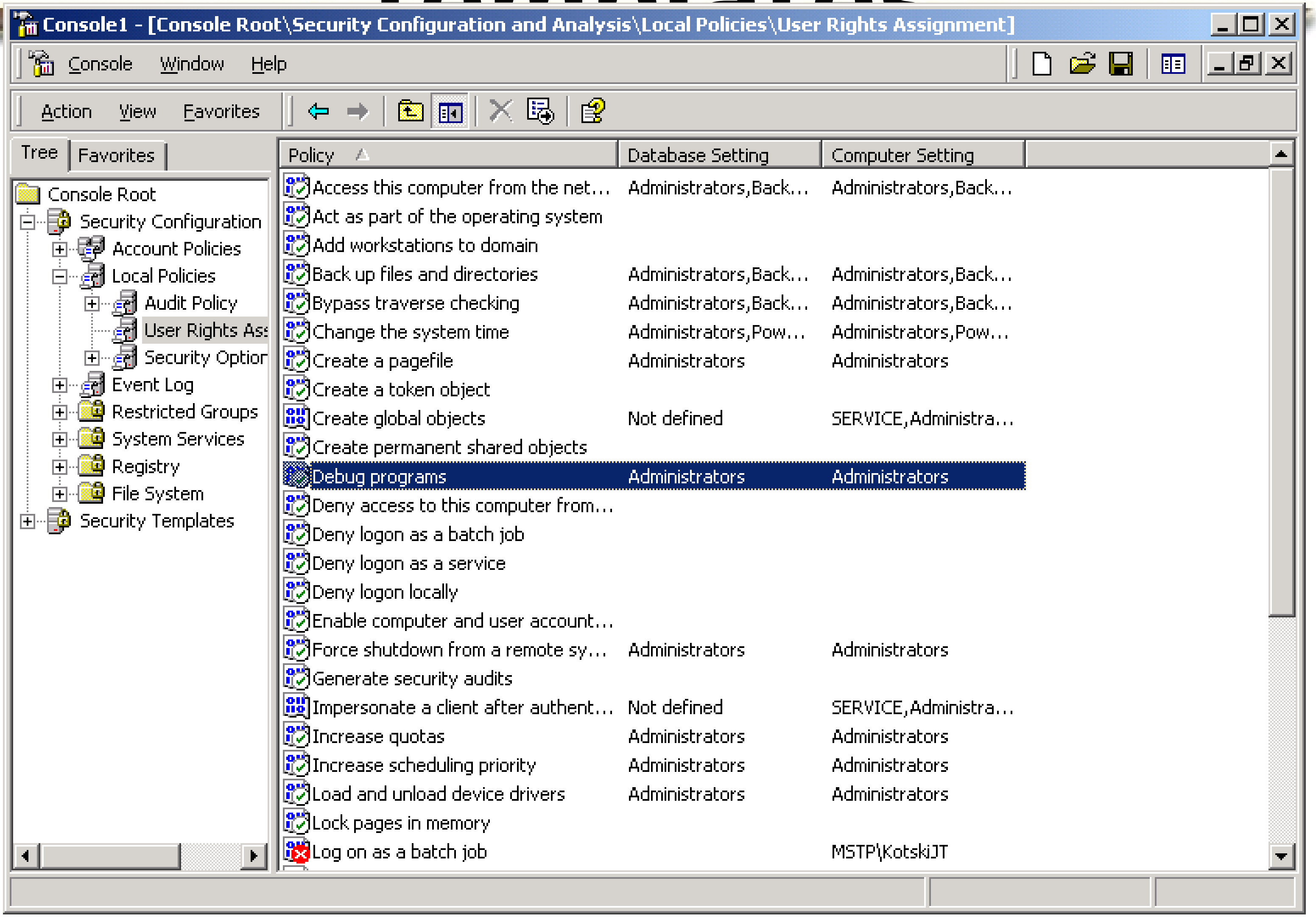
policies
basicdc.inf
basicsv.inf
basicwk.inf
compatws.inf
hisecdc.inf
hisecws.inf
ocfiless.inf
ocfilesw.inf
securedc.inf
securews.inf
setup security.inf

File name: *.inf

Files of type: Security Template (.inf)

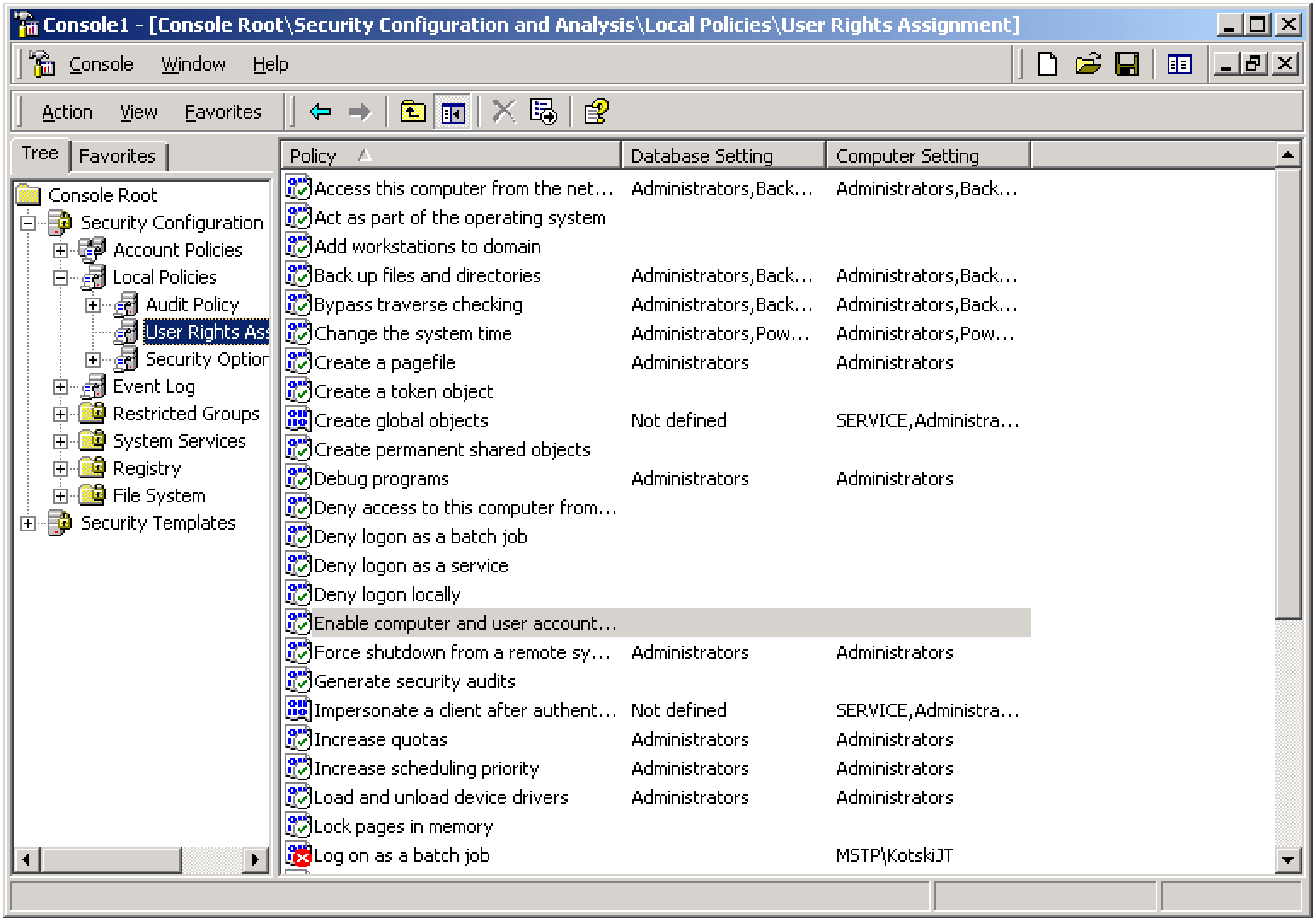
□ Clear this database before importing

Editing and creating templates



Policy	Database Setting	Computer Setting
Access this computer from the net…	Administrators,Back…	Administrators,Back…
Act as part of the operating system		
Add workstations to domain		
Back up files and directories	Administrators,Back…	Administrators,Back…
Bypass traverse checking	Administrators,Back…	Administrators,Back…
Change the system time	Administrators,Pow…	Administrators,Pow…
Create a pagefile	Administrators	Administrators
Create a token object		
Create global objects	Not defined	SERVICE,Administra…
Create permanent shared objects		
Debug programs	Administrators	Administrators
Deny access to this computer from…		
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user account…		
Force shutdown from a remote sy…	Administrators	Administrators
Generate security audits		
Impersonate a client after authent…	Not defined	SERVICE,Administra…
Increase quotas	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory		
Log on as a batch job		MSTP\KotskiJT

Editing and creating templates



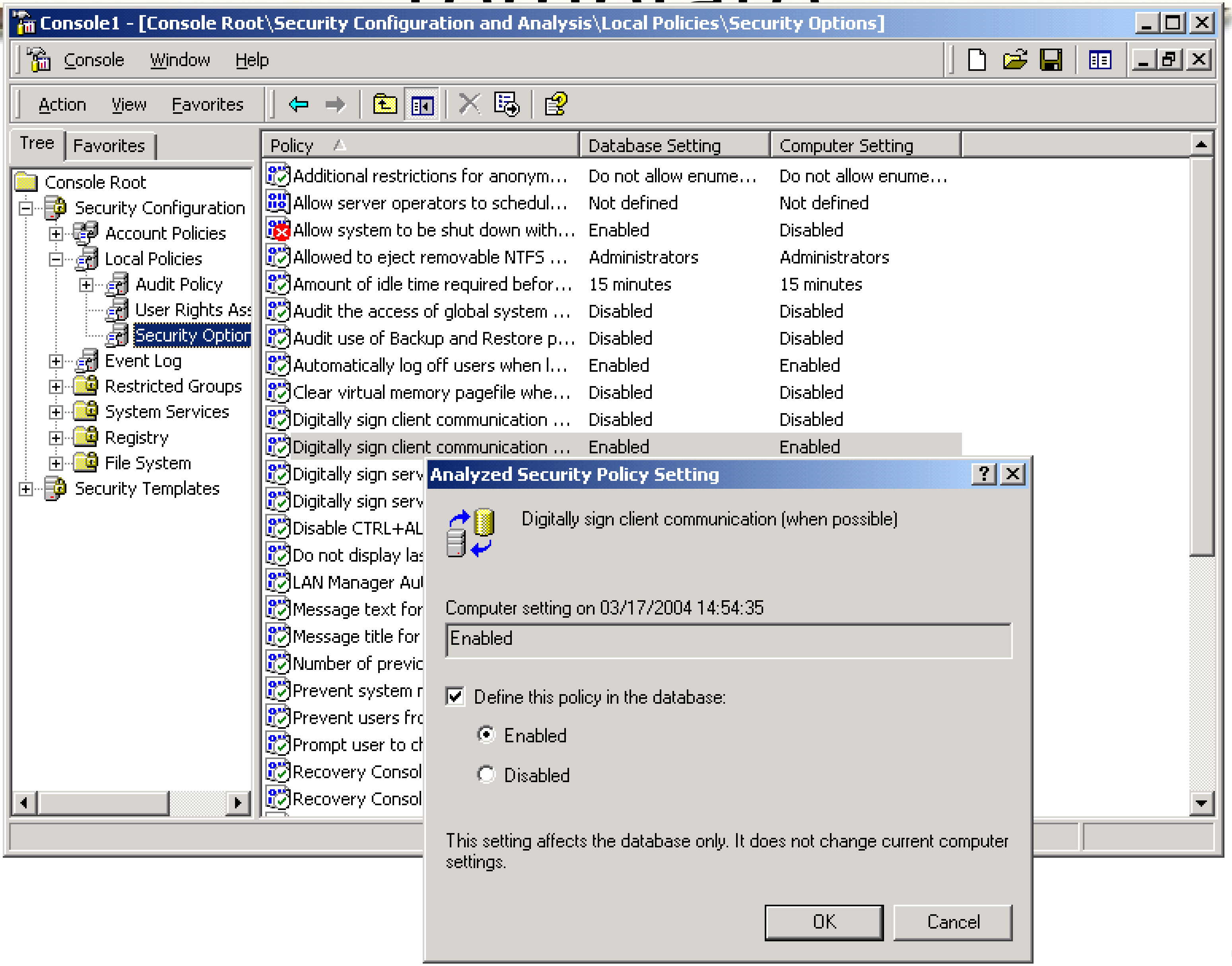
Policy	Database Setting	Computer Setting
Access this computer from the net...	Administrators,Back...	Administrators,Back...
Act as part of the operating system		
Add workstations to domain		
Back up files and directories	Administrators,Back...	Administrators,Back...
Bypass traverse checking	Administrators,Back...	Administrators,Back...
Change the system time	Administrators,Pow...	Administrators,Pow...
Create a pagefile	Administrators	Administrators
Create a token object		
Create global objects	Not defined	SERVICE,Administra...
Create permanent shared objects		
Debug programs	Administrators	Administrators
Deny access to this computer from...		
Deny logon as a batch job		
Deny logon as a service		
Deny logon locally		
Enable computer and user account...		
Force shutdown from a remote sy...	Administrators	Administrators
Generate security audits		
Impersonate a client after authent...	Not defined	SERVICE,Administra...
Increase quotas	Administrators	Administrators
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory		
Log on as a batch job		MSTP\KotskiJT

Define Templates

Policies in a template can be defined or undefined:

- When a policy is defined in the template, the policy’s value overwrites a computer’s local policy setting when the template is applied to that computer.
- When a policy is undefined in the template, a computer’s local policy setting remains in effect when the template is applied to that computer.

Defining a policy in a template



Console1 - [Console Root\Security Configuration and Analysis\Local Policies\Security Options]

Policy	Database Setting	Computer Setting
Additional restrictions for anonym…	Do not allow enume…	Do not allow enume…
Allow server operators to schedul…	Not defined	Not defined
Allow system to be shut down with…	Enabled	Disabled
Allowed to eject removable NTFS …	Administrators	Administrators
Amount of idle time required befor…	15 minutes	15 minutes
Audit the access of global system …	Disabled	Disabled
Audit use of Backup and Restore p…	Disabled	Disabled
Automatically log off users when l…	Enabled	Enabled
Clear virtual memory pagefile whe…	Disabled	Disabled
Digitally sign client communication …	Disabled	Disabled
Digitally sign client communication …	Enabled	Enabled
Digitally sign serv		
Digitally sign serv		
Disable CTRL+AL		
Do not display las		
LAN Manager Aut		
Message text for		
Message title for		
Number of previc		
Prevent system r		
Prevent users frc		
Prompt user to ch		
Recovery Consol		
Recovery Consol		

Analyzed Security Policy Setting

Digitally sign client communication (when possible)

Computer setting on 03/17/2004 14:54:35

Enabled

☑ Define this policy in the database:

● Enabled

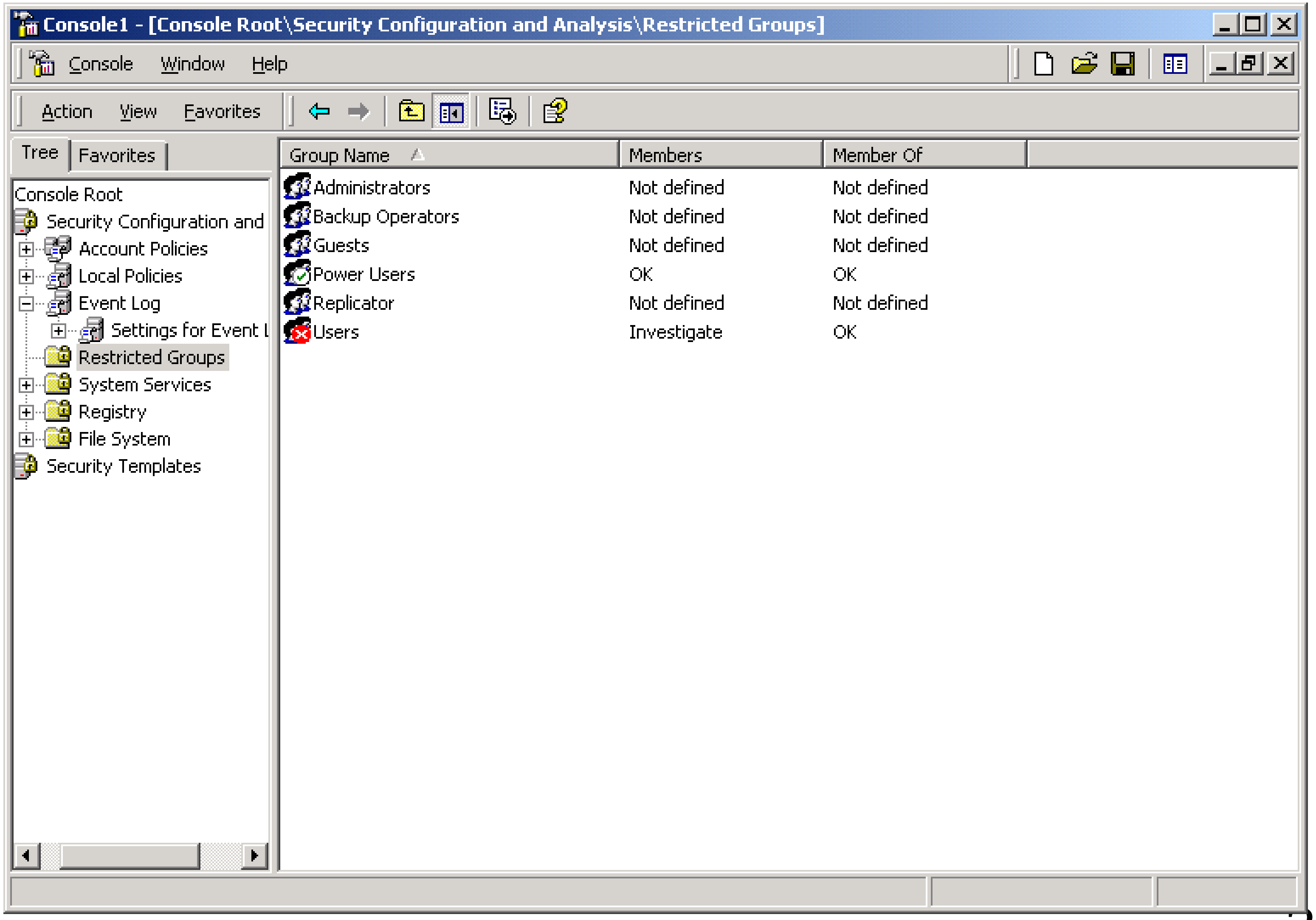
○ Disabled

This setting affects the database only. It does not change current computer settings.

Security Configuration and Analysis

- **Import security templates.** You must import at least one security template into the analysis database.
- **Clear database prior to import.** When you import a template, you can tell Security Configuration and Analysis to clear its database prior to the import.
- **Analyze your system.** Security Configuration and Analysis compares your computer’s policy settings to the ones currently in the analysis database.

Reviewing analysis results



Group Name	Members	Member Of
Administrators	Not defined	Not defined
Backup Operators	Not defined	Not defined
Guests	Not defined	Not defined
Power Users	OK	OK
Replicator	Not defined	Not defined
Users	Investigate	OK

Note the icons next to each policy.

These icons indicate whether or not the policy, as defined in the database, is active on your computer. The icons are as follows:

- A red "X" indicates that the policy values on your computer do not match those in the database.
- A green checkmark indicates that the policy values on your computer match the ones in the database.
- A **question mark** indicates that the policy is not defined in the database and was therefore not analyzed.
- An **exclamation point** indicates that the policy exists in the database and does not exist on your computer.
- **Edit the database.** You can double-click any of the policy settings in the database to change their values. Your edits affect only the database, not the policies on your computer.
- **Configure your system.** This task applies the values in the analysis database to your computer's local policies. To perform this task, right-click Security Configuration and Analysis and select Configure Computer Now from the pop-up menu.

Secedit.exe

- **Secedit /analyze** performs an analysis. You must specify an existing security database file using the **/db** parameter—for example, **Secedit /analyze /db mysec.sdb.**
- **Secedit /configure** configures your computer with a security template. You must specify a security database using the **/db** parameter.
- **Secedit /export** exports the security settings on your computer into a template file. You must specify the output filename.
- **Secedit /validate** compares your computer to an existing template and reports on any differences.

REVIEW

You learned how the Security Configuration Manager (SCM) consists of several tools that can help you manage computers’ security policies and other security settings. The Security Templates snap-in enables you to modify and create security templates, which can be applied to computers. Security Configuration and Analysis enables you to view templates’ settings and view the result of multiple overlapping templates. Security Configuration and Analysis also enables you to apply a set of templates to your computer. **Secedit.exe** duplicates most of Security Configuration and Analysis’ key functionality but works from a command line, enabling you to perform analysis and configuration tasks from batch files.

MAGTF STAFF TRAINING PROGRAM

DOCEMUS PRIMAM ACIEM

TCP/IP Brief

TCP/IP

Networking with TCP/IP

- How computers communicate by using TCP/IP
- How to configure Windows TCP/IP
- How to calculate subnet masks

How TCP/IP Works

You program a computer with the following TCP/IP parameters:

✓ An IP address that is unique on your network

✓ A subnet mask

✓ The IP address of a default gateway

✓ The IP address of a name resolution server

Sending the data

- TCP/IP checks to see if it knows the IP address for the remote computer.
  - If it doesn’t, it contacts a name resolution server and asks that server to translate the computer name into an IP address.
- TCP/IP uses its subnet mask to determine whether or not the remote computer is on the same *subnet*.
  - A subnet is a single network that uses a single range of IP addresses.

Sending the data

- If TCP/IP determines that the remote computer is on the same subnet, it follows these steps:
  - TCP/IP sends out a special query using the Address Resolution Protocol (ARP).
  - The computer using the IP address in the ARP query responds:
    - The computer includes its physical address in the reply. The physical address, also called a Media Access Control (MAC) address, is burned into the computer’s network interface card (NIC) by the manufacturer.
- TCP/IP receives the ARP reply. TCP/IP now knows the remote computer’s MAC address and can send data directly to the remote computer.

Remote computer

- If TCP/IP determines that the remote computer is not on the same subnet, it follows these steps:
  - **1.** TCP/IP sends the data destined for the remote computer to the default gateway you configured.
  - **2.** The default gateway is usually a network hardware device called a *router*, which is capable of connecting multiple subnets together

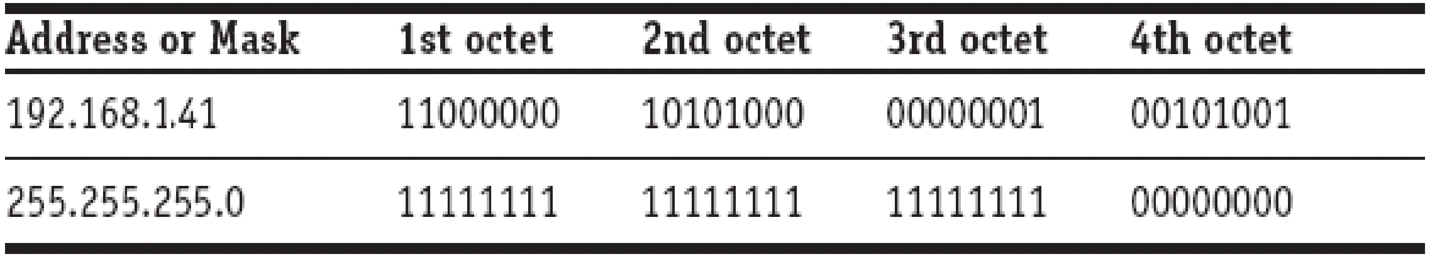
Subnets and subnet masks

- TCP/IP has to perform is determining whether or not a given IP address is on the same subnet.
  - An IP address looks something like this: 192.168.1.52
  - A portion of the IP address is called the *network ID* and acts as a unique identifier for a particular subnet.
  - The rest of the IP address is called the *host ID* and uniquely identifies a particular computer or network device on that subnet.
- How can you tell which part of the IP address is which?
  - By using the subnet mask. A subnet mask looks a lot like an IP address, with four groups of numbers: 255.255.255.0.

Binary Conversion

Computers are binary devices that can think only in zeros and ones

- Convert each of the four groups (called *octets*) of numbers into binary. For example, an IP address of 192.168.1.41 and a subnet mask of 255.255.255.0 look like this in binary:



Address or Mask	1st octet	2nd octet	3rd octet	4th octet
192.168.1.41	11000000	10101000	00000001	00101001
255.255.255.0	11111111	11111111	11111111	00000000

Everyplace you see a “1” in the subnet mask corresponds to the portion of the IP address that is the network ID. Everyplace you see a “0” in the subnet mask corresponds to the portion of the IP address that is the host ID. So, in this example, the network ID is 192.168.1, and the host ID is 41.

Basic TCP/IP Services

- **Data transmission.** Handled by two protocols: the User Datagram Protocol (UDP) and the Transport Control Protocol (TCP).
- **Name resolution.** Provided by the Domain Name System, or DNS, protocol.
- **Windows Internet Name System (WINS).** Older versions of Windows also use WINS to translate computer names into IP addresses.
  - Windows Server 2003 is compatible with WINS
- **Address Resolution Protocol (ARP).** Provides address resolution.
- **IP configuration.** Provided by the Dynamic Host Configuration Protocol, or DHCP.
- **Application services.** Such as Web servers and file transfer servers. Each application uses a different TCP/IP protocol to accomplish its task.

Designing services into a network

- The basic TCP/IP services (WINS, DNS, and DHCP) aren’t automatically included in a network because you usually install them on only one or two servers.
  - Most organizations include two DNS servers on their network, so that if one stops working, the other can continue servicing name resolution requests.
  - Most organizations also include two DHCP servers on their network, although you have to be careful with that scenario
    - Organizations usually configure the two DHCP servers to each issue separate ranges of valid IP addresses.
- Most of the basic TCP/IP services can all be installed on a single pair of servers, so that each server runs DNS, WINS, DHCP, and perhaps a Web or FTP server.

TCP/IP services and Windows Server 2003

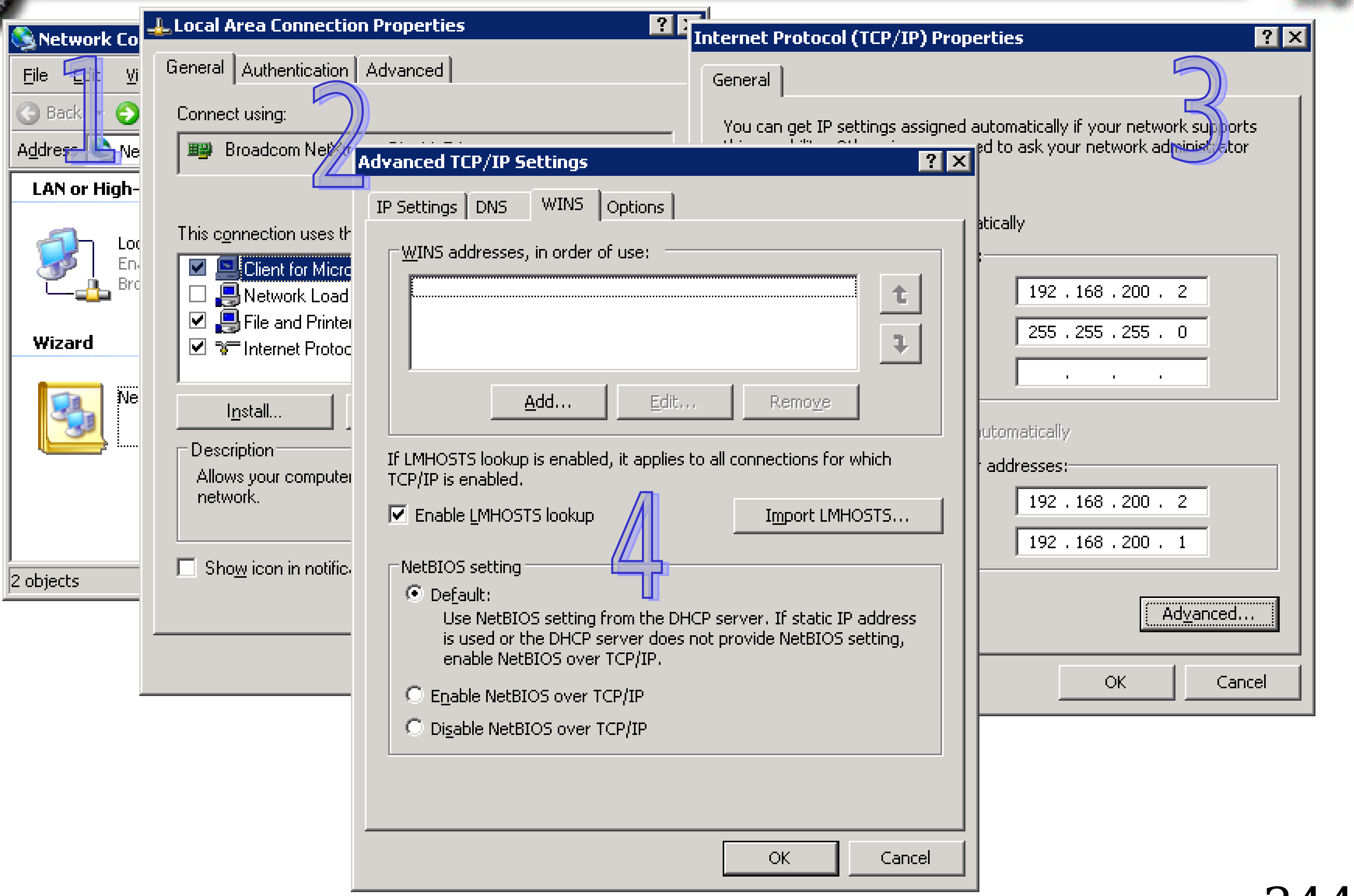
- Some companies run their DNS and DHCP servers on UNIX-based computers.
- Windows Server 2003 includes the software necessary to provide all of the basic TCP/IP services to your network, so you don’t need to purchase any other operating systems.
  - To install any of the basic TCP/IP services, just run the Add/Remove Programs utility from the Control Panel.

TCP/IP services and W2K3

Select the Add/Remove Windows Components option, and then select the service you want to install:

- To install a Web server or FTP server, select Internet Information Services (IIS). Modify the IIS installation option to include a Web server, FTP server, or both, as appropriate.
- To install a DHCP server, select DHCP Service from the Networking options.
- To install a WINS server, select WINS Service from the Networking options.
- To install a DNS server, select DNS Service from the Networking options.
  - After installing a TCP/IP service on Windows Server 2003, you have to configure the service.

Configuring TCP/IP



Local Area Connection Properties

General | Authentication | Advanced

Connect using:

Broadcom Net

This connection uses th

☑ Client for Micro
□ Network Load
☑ File and Printe
☑ Internet Protoc

Install...

Description

Allows your computer network.

□ Show icon in notific

Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports ... ed to ask your network administrator

atically

192 . 168 . 200 . 2

255 . 255 . 255 . 0

. . .

utomatically

addresses:

192 . 168 . 200 . 2

192 . 168 . 200 . 1

Advanced...

OK | Cancel

Advanced TCP/IP Settings

IP Settings | DNS | WINS | Options

WINS addresses, in order of use:

Add... | Edit... | Remove

If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.

☑ Enable LMHOSTS lookup

Import LMHOSTS...

NetBIOS setting

● Default:
Use NetBIOS setting from the DHCP server. If static IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.

○ Enable NetBIOS over TCP/IP

○ Disable NetBIOS over TCP/IP

OK | Cancel

REVIEW

You learned how computers use TCP/IP to communicate over a network. You also learned how TCP/IP works, and how the basic TCP/IP services provide the necessary features for TCP/IP to function on a network. You learned how Windows Server 2003 provides the necessary software to implement the basic TCP/IP services, and you learned how to configure the TCP/IP settings on a Windows Server 2003.